ABSTRACT

In this thesis, we prove that the subvarieties of $\underline{\underline{A}}_m(\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_n)$ are CREAM in the sense of Higman [15] when m, n are coprime and n is an odd integer not divisible by q^4 for any prime q. In our methods of investigation, we also have occasion to solve the isomorphism problem for finite q-groups of nilpotency class 2 with cyclic centre when q is an odd prime. This enables us to classify the closed classes of irreducible linear groups over GF(p) belonging to $\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_{q^i}$, $i \geq 1$, where p is a prime different from q. The structure of non-degenerate alternating forms on modules over the ring of integers modulo q^α, $\alpha \geq 1$, are studied and used to calculate the group of linear automorphisms of a finite q-group of class 2 with cyclic centre.

THE CREAM CONJECTURE
AND CERTAIN
ABELIAN-BY-NILPOTENT VARIETIES

by

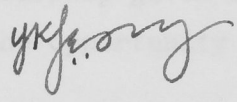
LEONG, YU KIANG

A thesis submitted to the
Australian National University
for the degree of
Doctor of Philosophy

Canberra, June 1972

Statement

Unless stated otherwise, the results in this thesis are my original work.



ACKNOWLEDGEMENTS

I thank

Dr R.A. Bryce, my supervisor, for suggesting the research problem for this thesis, for the helpful discussions during the past three years and, above all, for the criticism, patience and care with which he read the preliminary drafts of this thesis;

Dr L.G. Kovács, my co-supervisor, for his generous help so invaluable during these formative years;

Dr M.F. Newman for making available to me a preprint of D.L. Winter and for the interest he has shown in my work;

Dr J.M. Brady and Dr John Cook for making available to me copies of their Ph.D. theses;

Mrs Barbara Geary for her work in typing this thesis.

I am grateful for the Research Scholarship given by the Australian National University which has given me the opportunity to widen my perspective of life and mathematics.

CONTENTS

CHAPTER 0

INTRODUCTION

The present work has arisen from an attempt to confirm the claim (now withdrawn) by Brady, Bryce and Cossey [4] that the subvarieties of $\underline{\underline{A}}_m(\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_n)$ are CREAM, where m, n are coprime, in the sense of Higman [15]. This attempt has succeeded for certain values of n, namely when n is odd and not divisible by q^4 for any prime q. In the course of the work we are led into by-ways of independent interest.

The history of the CREAM question is a short and sparse one. In 1965, Graham Higman [15] brought up some questions concerning the analytic form of the function $n \mapsto F_n(\underline{\underline{V}})$ for a locally finite variety $\underline{\underline{V}}$. On the evidence of some varieties and classes of varieties, he was led to introduce a class of functions which he called CREAM and to conjecture that $n \mapsto F_n(\underline{\underline{V}})$ is CREAM for every locally finite variety $\underline{\underline{V}}$. To my knowledge the only work done directly on CREAM since Higman's original lecture is in the thesis of John Cook [5]. Both Higman and Cook prove results of the sort that a CREAM variety remains CREAM if finitely many critical groups are adjoined to it. In this sense, we break new ground: infinitely many of the varieties we prove to be CREAM are not the join of a proper subvariety and a Cross variety.

We begin Chapter 1 with a section (1.1) to clarify and make precise at the outset Higman's definition of CREAM functions and CREAM varieties. Some properties of the class of CREAM functions are given: in particular, the class of CREAM functions is countable. In the light of the known existence of uncountably many locally finite varieties (O'lšanskiĭ [22]), Theorem 1.1.5 tells us that Higman's CREAM conjecture cannot be true. Still it is of interest to know which varieties are CREAM. The rest of Chapter 1 is an elaboration of the methods sketched by Higman [15] to study the CREAM question for subvarieties of $\underline{\underline{A}}_m\underline{\underline{W}}$. With the help of representation theory, the problem is reduced to an investigation of a certain function $C_{\underline{\underline{X}}}$ associated with a closed class $\underline{\underline{X}}$ of irreducible linear groups belonging to $\underline{\underline{W}}$. Our work is essentially an application of his

methods to the case when $\underline{\underline{W}} = \underline{\underline{N}}_2 \wr \underline{\underline{B}}_n$. To do this we need extensive information about finite q-groups of class 2 with cyclic centre.

The finite q-groups of class 2 with cyclic centre have been explicitly described in Brady, Bryce and Cossey [4]. Based on this description, Chapter 2 solves the isomorphism problem for such groups with q odd, and assigns to each of these groups a set of invariants. The methods used are elementary. In 2.1 we discuss central products with cyclic centre, and in 2.2 we study how a q-group of class 2 with cyclic centre can decompose as a central product of centrally indecomposable factors. This enables us to obtain a certain canonic decomposition. The proof of its uniqueness occupies the whole of 2.3. (Whether analogous methods can be developed to solve the isomorphism problem for finite 2-groups of class 2 with cyclic centre I have not investigated.) The existence and uniqueness theorems proved in Chapter 2 are of interest quite apart from the use we put them to later and should be compared with the results of M.F. Newman [21], C.Y. Tang [24] and M. Schick [23].

In Chapter 3 we give a classification of the closed classes of irreducible linear groups over $GF(p)$ belonging to $\underline{\underline{N}}_2 \wr \underline{\underline{B}}_{q^n}$ where p, q are different primes. We rely heavily on results of Brady, Bryce and Cossey [4] concerning such linear groups. As shown in 3.1, it suffices to consider these linear groups over a suitable splitting field. In 3.2 we investigate in some detail the linear factors of the irreducible linear groups under consideration. The closed classes are then classified by an inductive process in 3.3. This is applied to prove some results on the lattice of subvarieties of $\underline{\underline{A}}_p\left(\underline{\underline{N}}_2 \wr \underline{\underline{B}}_{q^n}\right)$.

The main aim of Chapter 4 is to calculate the order of the group of linear automorphisms, lin aut G , of a finite q-group G of class 2 with cyclic centre, q odd. By a familiar technique, we can consider $G/Z(G)$ as a module U over Z_{q^m} (the ring of integers modulo q^m) with an alternating form defined on it. It turns out that lin aut G is closely related to a certain subgroup $QSp(U)$ of the group of isometries $Sp(U)$ of U . However the structure of alternating forms on a module over a ring with zero divisors does not seem to have been well-studied. Consequently it is necessary to study

in some detail in 4.1 the concept and structure of a non-degenerate symplectic module U over Z_{p^m}, analogous to that of a non-degenerate symplectic vector space (Huppert [16]). With the structure of U known, we can then calculate in 4.2 the order of $QSp(U)$ by a systematic enumeration of "quasi-hyperbolic pairs", from which the bulk of the calculations arise. In 4.3 we find that the description of $QSp(U)$ in certain cases is sufficient to yield extensions of some results of Winter [26].

Chapter 5 is devoted to a study of the CREAM problem for subvarieties of $\underline{\underline{A}}_p\left(\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_{q\,i}\right)$. In principle we can calculate the function $C_{\underline{\underline{X}}}$, mentioned in the third paragraph, for any closed class $\underline{\underline{X}}$ of irreducible linear groups in $\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_{q\,i}$ using the results of Chapter 4. But the apparently formidable expressions obtained force us to restrict our attention to the case when $i \leq 3$. To show that $C_{\underline{\underline{X}}}$ is CREAM, we have firstly to classify the infinite classes of irreducible linear groups of a fixed exponent in $\underline{\underline{X}}$ and then to collect these into finitely many classes $\underline{\underline{S}}$ such that $C_{\underline{\underline{S}}}$ is CREAM : 5.1 is directed towards this purpose. In 5.2, C_X is calculated explicitly for certain linear groups X relevant to the case under consideration. In 5.3 we gather all the available machinery to solve in the affirmative the CREAM problem in our restricted case. Finally, lest it be thought that an affirmative answer to CREAM is inevitable, we give in 5.4 an example of an infinite class $\underline{\underline{S}}$ of groups of exponent q^4 which is not closed but for which $C_{\underline{\underline{S}}}$ is not CREAM.

In this thesis we will freely use known results in the theories of groups, varieties of groups and representation of groups, including some elementary results of real-valued functions which are used in 5.4. The completion of a proof of a theorem, lemma or corollary will be indicated by // . The notations used in this thesis may vary from chapter to chapter, but it will be clear at the beginning of each chapter as to what the changes in notations are. However the following notations will be used consistently throughout this thesis.

$\mathbb{R}$, the real numbers

Q^+ , the positive rational numbers

N^+ , the positive integers

p, q , prime numbers

f, g , functions $R \to R$

X, Y , classes of functions $R \to R$

$\mathrm{GF}(p)$, the field of p elements, p a prime

E, F, L, K , fields

$K(\omega)$, the field obtained by adjoining ω to K

$\mathrm{GL}(n, K)$, the general linear group of degree n over K

$|S|$, the order of a group or set S

$|x|$, the order of an element x of a group

$H \leq G$, H is a subgroup of G

$H < G$, H is a proper subgroup of a group G

$H \lhd G$, H is a normal subgroup of a group G

$Z(G)$, the centre of a group G

G' , the derived group of a group G

$$x^y = y^{-1}xy$$

$$[x, y] = x^{-1}y^{-1}xy$$

$$[x, y, z] = \big[[x, y], z\big]$$

$\langle x_1, \ldots, x_r \rangle$, the group generated by $x_1, \ldots, x_r$

$\Phi(G)$, the Frattini subgroup of a group G

$\mathrm{aut}\ G$, the group of automorphisms of a group G

$\mathrm{inn}\ G$, the group of inner automorphisms of a group G

X, Y, Z , irreducible linear groups

$\underline{\underline{X}}, \underline{\underline{Y}}, \underline{\underline{Z}}$, classes of irreducible linear groups

$Y \prec\!\!\!\cdot\, X$, Y is a linear factor of X

$\mathrm{lin\ aut}\ X$, the group of linear automorphisms of X

$U \oplus V$, the direct sum of the modules U, V

$\ker U$, $\{x \in G : ux = u \text{ for all } u \in U\}$ where U is a KG-module

$U \# V$, the outer tensor product of the modules U, V

$F_n(\underline{\underline{V}})$, the free group of rank n of a variety $\underline{\underline{V}}$

$\underline{\underline{A}}_m$, the variety of abelian groups of exponent dividing m

$\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_n$, the variety of nilpotent groups of class ≤ 2 and exponent dividing n .

CHAPTER 1

SOME REMARKS ON A PAPER OF GRAHAM HIGMAN

In this chapter, we will elaborate on the observations and remarks made in Sections 2.1, 2.2, 2.4 and 2.5 of Graham Higman's paper [15].

1.1 CREAM functions and CREAM varieties

In this section, we denote the real numbers by $\mathbb{R}$ and the positive rational numbers by Q^+. If f and g are two functions such that the range of g is in the domain of f, we write $f \circ g$ for the composite function $f \circ g : x \mapsto f(g(x))$ for every x in the domain of x.

Let X be a class of functions $\mathbb{R} \to \mathbb{R}$. Define the following operations P_h and E_b on X. If h is a rational polynomial function $\mathbb{R}^r = \underbrace{\mathbb{R} \times \ldots \times \mathbb{R}}_{r} \to \mathbb{R}$, and $g_1, \ldots, g_r \in X$, then let $(g_1, \ldots, g_r) = \mathbb{R} \to \mathbb{R}^r$ be defined by

$$(g_1, \ldots, g_r) : x \mapsto (g_1(x), \ldots, g_r(x)) .$$

Put

$$P_h X = \{h \circ (g_1, \ldots, g_r) : g_1, \ldots, g_r \in X\} .$$

If $b \in Q^+$ and $f \in X$, then let $b^f = \mathbb{R} \to \mathbb{R}$ be defined by

$$b^f = x \mapsto b^{f(x)} .$$

Put

$$E_b X = \{b^f : f \in X\} .$$

We call a class X of functions $\mathbb{R} \to \mathbb{R}$ closed if

$$P_h X \subseteq X , \quad E_b X \subseteq X$$

for all rational polynomial functions h and every $b \in Q^+$.

1.1.1 LEMMA. *A closed class of functions is closed under addition and multiplication of functions.*

Proof. Let X be a closed class of functions $\mathbb{R} \to \mathbb{R}$. Let $g_1, g_2 \in X$, and write $g = g_1 + g_2$. Define the rational polynomial function $h : \mathbb{R}^2 \to \mathbb{R}$ by $h : (x, y) \to x + y$. Then clearly $g = h \circ (g_1, g_2) \in X$. If f is the function $\mathbb{R} \to \mathbb{R}$ given by $f : x \mapsto g_1(x)g_2(x)$, then define the rational polynomial function $k : \mathbb{R}^2 \to \mathbb{R}$ by $k : (x, y) \mapsto xy$. Clearly $f = k \circ (g_1, g_2) \in X$. //

The class of all functions $\mathbb{R} \to \mathbb{R}$ is evidently closed, and the intersection of closed classes is again closed. Thus, to each class X, there is a smallest closed class containing X, called the *closure* of X which we denote by CREAM X.

A number of facts about the closed classes will be useful.

1.1.2 LEMMA. *If X is countable, then* CREAM X *is countable.*

Proof. Let

$$X^{(1)} = \cup A_1 \dots A_r X_\alpha ,$$

where $A_1 \dots A_r X_\alpha = A_1(A_2 \dots A_r)X_\alpha$ inductively, and the union is taken over all such terms where $A_1, \dots, A_r$ are of the form P_h or E_b, and X_α is a finite subset of X. We allow $r = 0$, in which case $A_0 X_\alpha = X_\alpha$. We define $X^{(i)}$ inductively for $i > 1$ as follows.

$$X^{(i)} = \cup A_1 \dots A_r X_\alpha^{(i-1)} ,$$

where the union is taken over all such terms where $A_1, \dots, A_r$ are of the form P_h or E_b and $X_\alpha^{(i-1)}$ is a finite subset of $X^{(i-1)}$.

The closure of X is then given by CREAM $X = \bigcup_{i=1}^{\infty} X^{(i)}$.

Denoting the union on the right by Y, we show that Y is closed. First, note that $X^{(i-1)} \subseteq X^{(i)}$. Let $h : \mathbb{R}^s \to \mathbb{R}$ be a rational polynomial function, and let $g_1, \dots, g_s \in Y$. Then $g_1, \dots, g_s \in X^{(k)}$ for some $k \geq 1$. In fact,

$$g_i \in A_{j1} \dots A_{j,r_j} X_{\alpha_j}^{(k-1)} , \quad j = 1, \dots, s .$$

Put

$$X_\beta^{(k-1)} = \bigcup_{j=1}^{s} A_{j1} \dots A_{j,r_j} X_{\alpha_j}^{(k-1)} ,$$

so that $X_\beta^{(k-1)}$ is finite. Then

$$h \circ \{g_1, \dots, g_r\} \in P_h X_\beta^{(k-1)} \subseteq X^{(k)} .$$

Hence $P_h Y \subseteq Y$.

Next, let $b \in Q^+$, $f \in Y$. Then $f \in X^{(i)}$ for some i , and so $f \in A_1 \dots A_r X_\alpha^{(i-1)}$ for some $A_1, \dots, A_r$. Hence

$$b^f \in E_b\left(A_1 \dots A_r X_\alpha^{(i-1)}\right) = E_b A_1 \dots A_r X_\alpha^{(i-1)} \subseteq X^{(i)} .$$

Then Y is closed. Moreover Y contains X and is contained in the closure of X .

Finally we prove that each $X^{(i)}$ is countable. Since the family of all finite subsets of a countable set is countable, the collection of terms of the form $A_1 \dots A_r X_\alpha$ is countable. Each of these terms is a finite set, and so $X^{(1)}$ is countable. It follows easily by induction on i that $X^{(i)}$ is countable for all $i \geq 1$. Hence CREAM X is countable. //

Let j be the identity function $\mathbb{R} \to \mathbb{R}$. We denote CREAM $\{j\}$ by CREAM . A function in CREAM is called a CREAM function. We shall need the following property of CREAM .

1.1.3 LEMMA. *The class* CREAM *is closed under composition of functions.*

Proof. By Lemma 1.1.2, CREAM $= \bigcup_{i=1}^{\infty} X^{(i)}$, where $X^{(i)} = \bigcup A_1 \dots A_r X_\alpha^{(i-1)}$, $X_\alpha^{(0)} = X_\alpha$. First we show that if $f \in X^{(1)}$, $g \in$ CREAM , then $f \circ g \in$ CREAM . Now $f = A_1 \dots A_r\{j\}$

for some finite sequence of the operations P_h, E_b, say $A_1, \ldots, A_r$. We use induction on r. If $r = 0$, then $f \circ g = j \circ g = g \in \text{CREAM}$. Suppose therefore that $r > 0$, and that if $h = A_2 \ldots A_r\{j\}$, then $h \circ k \in \text{CREAM}$ for every $k \in \text{CREAM}$. Now if $A_1 = E_b$ for some $b \in Q^+$, then

$$f \circ g = b^h \circ g = b^{h \circ g} \in E_b\{h \circ g\} \subseteq E_b \text{ CREAM} \subseteq \text{CREAM},$$

where $h = A_2 \ldots A_r\{j\}$. If $A_1 = P_h$ for some rational polynomial function h, then $f = h \circ k$, where $k = A_2 \ldots A_r\{j\}$, and hence

$$f \circ g = (h \circ k) \circ g = h \circ (k \circ g) \in P_h \text{ CREAM} \subseteq \text{CREAM},$$

since $k \circ g \in \text{CREAM}$ by the induction hypothesis.

We use induction on i to show that if $f \in X^{(i)}$, $g \in \text{CREAM}$, then $f \circ g \in \text{CREAM}$. This is true for $i = 1$. So we assume that $i > 1$ and that if $f \in X^{(i-1)}$, then $f \circ g \in \text{CREAM}$ for all $g \in \text{CREAM}$. Let $f \in X^{(i)}$ so that $f \in A_1 \ldots A_r X_\alpha^{(i-1)}$. We use induction on r. If $r = 0$, then $f \in X^{(i-1)}$ and so, by assumption, $f \circ g \in \text{CREAM}$. Suppose then that $r > 0$ and that if $h \in A_2 \ldots A_r X_\alpha^{(i-1)}$, then $h \circ k \in \text{CREAM}$ for every $k \in \text{CREAM}$. If $A_1 = E_b$ for some $b \in Q^+$, then

$$f \circ g = b^h \circ g = b^{h \circ g} \in E_b\{h \circ g\} \subseteq E_b \text{ CREAM} \subseteq \text{CREAM},$$

where $h \in A_2 \ldots A_r X_\alpha^{(i-1)}$. If $A_1 = P_h$ for some rational polynomial function h, then there exist $g_1, \ldots, g_s \in A_2 \ldots A_r X_\alpha^{(i-1)}$ such that $f = h \circ (g_1, \ldots, g_s)$. Thus

$$f \circ g = [h \circ (g_1, \ldots, g_s)] \circ g = h \circ [(g_1, \ldots, g_s) \circ g] = h \circ (g_1 \circ g, \ldots, g_s \circ g).$$

But by the induction hypothesis on r, $g_i \circ g \in \text{CREAM}$ for $i = 1, \ldots, s$, and hence $f \circ g \in P_h \text{ CREAM} \subseteq \text{CREAM}$. //

We now relate the foregoing discussion to varieties of groups. Let $\underline{\underline{V}}$ be a locally finite variety, and let $F_n(\underline{\underline{V}})$ be the free group of rank n of $\underline{\underline{V}}$. Let N^+ denote the positive integers. We say that $\underline{\underline{V}}$ is CREAM if the function $N^+ \to \mathbb{R}$ defined by $n \mapsto |F_n(\underline{\underline{V}})|$ is the restriction to N^+ of a CREAM function.

At this stage, it is perhaps worth proving the following simple theorems to illustrate the use of CREAM functions.

1.1.4 THEOREM. *The product of* CREAM *varieties is* CREAM .

Proof. Suppose that $\underline{\underline{V}}$, $\underline{\underline{W}}$ are CREAM varieties with the corresponding CREAM functions f, g respectively. Now, by 21.13 of Hanna Neumann [20],

$$|F_n(\underline{\underline{V}}\ \underline{\underline{W}})| = |F_m(\underline{\underline{V}})|.|F_n(\underline{\underline{W}})| = f(m)g(n) ,$$

where $m = (n-1)g(n) + 1$.

The function $j - 1$ is CREAM and therefore by Lemma 1.1.1, the function $(j-1)g + 1$ is CREAM . Hence, by Lemma 1.1.3, the function $f \circ \{(j-1)g+1\}$ is CREAM ; whence the function $h = [f \circ \{(j-1)g+1\}]g$ is CREAM by Lemma 1.1.1. But $h(n) = |F_n(\underline{\underline{V}}\ \underline{\underline{W}})|$ for every $n \in N^+$, and hence $\underline{\underline{V}}\ \underline{\underline{W}}$ is CREAM . //

As a consequence of Lemma 1.1.2 and a result of O'lšanskiĭ [22] that there are uncountably many locally finite varieties, we have the following theorem which seems to be well-known though no reference can be given.

1.1.5 THEOREM. *Not all locally finite varieties are* CREAM .

Proof. If not, then by Lemma 1.1.2, there is a CREAM function, f say, and uncountably many varieties $\underline{\underline{V}}$ such that

$$f(n) = |F_n(\underline{\underline{V}})| . \tag{1}$$

However, since a locally finite variety is uniquely determined by the set of its free groups of finite rank and since there are but finitely many isomorphism classes of groups of a given finite order, there can be at most countably many varieties satisfying (1). //

We conclude this section with a number of minor comments on the paper of Higman [15]. The definition of CREAM functions given in

this section is not exactly Higman's; he presumably has only functions $N^+ \to \mathbb{R}$ in mind. However, composition of CREAM functions is then impossible and to get it, one must consider functions $\mathbb{R} \to \mathbb{R}$. The definition of CREAM variety, though, is Higman's. It only needs checking that the restriction to N^+ of one of our CREAM functions is CREAM in Higman's sense.

With the notations in the proof of Lemma 1.1.3, let $f \in X^{(1)}$ so that $f = A_1 \ldots A_r\{j\}$. Use induction on r. If $r = 0$, then $f = j$ and so f restricted to N^+ is CREAM in Higman's sense. So suppose that $r > 0$ and that the restriction to N^+ of a function of the form $A_2 \ldots A_r\{j\}$ is CREAM in Higman's sense. If $A_1 = E_b$ for some $b \in Q^+$, then $f = b^g$ where $g = A_2 \ldots A_r\{j\}$. Hence, for every $n \in N^+$, $f(n) = b^{g(n)}$, and therefore the restriction of f to N^+ is CREAM in the sense of Higman. However, if $A_1 = P_h$ for some rational polynomial function h, then $f = h \circ g$, where $g = A_2 \ldots A_r\{j\}$. For every $n \in N^+$, $f(n) = h\big(g(n)\big)$ and hence the restriction of f to N^+ is CREAM in the sense of Higman. An induction on i then shows that, for every $f \in X^{(i)}$, $i \geq 1$, the restriction of f to N^+ is CREAM in Higman's sense. As the details are similar to those above, we omit them.

In his thesis, Cook [5] considered the CREAM conjecture for the varieties $\underline{\underline{V}} \vee \underline{\underline{W}}$ where $\underline{\underline{V}}$ is CREAM and $\underline{\underline{W}}$ is generated by a single critical group whose proper sections are all in $\underline{\underline{V}}$, and found that he needed an (apparently) wider class of functions than that of Higman. Roughly speaking, he makes CREAM division closed and also requires that it contains the functions f_n, for each $n \in N^+$, given by

$$f_n : x \mapsto \begin{cases} 1 , & x = n , \\ 0 , & x \neq n . \end{cases}$$

However, in our work on the variety $\underline{\underline{A}}_m\big(\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_n\big)$ where m, n are

coprime positive integers, we do not find it necessary to do this: Higman's original definition suffices.

1.2 The subvarieties of the variety $\underline{\underline{A_p W}}$

Higman [14] has characterized those varieties $\underline{\underline{V}}$ satisfying $\underline{\underline{W}} \leq \underline{\underline{V}} \leq \underline{\underline{A_p W}}$ where p is a prime not dividing the exponent of $\underline{\underline{W}}$, in terms of the closed classes of irreducible linear groups over $GF(p)$ belonging to $\underline{\underline{W}}$. We merely state his main result, Theorem 1.2.1 below, without proof.

We recall some definitions on linear groups. Let X and Y be linear groups acting on the vector spaces V and W (over some field F) respectively. Then X and Y are said to be *linearly isomorphic* if there is a bijective linear transformation $\gamma : V \to W$ such that $\gamma^{-1} X \gamma = Y$. If X and Y are considered as subgroups of the general linear group $GL(n, F)$, then it is a direct consequence of the definition that X and Y are linearly isomorphic if and only if they are conjugate in $GL(n, F)$.

Let X and Y be linear groups acting on the vector spaces V and W over $GF(p)$ respectively. Then Y is said to be a *linear factor* of X (and we write $Y \prec X$) if X has a subgroup X_0 and V has an X_0-admissible subspace V_0 such that the restriction of X_0 to V_0 is linearly isomorphic to Y. Now suppose that X and Y are irreducible linear groups, $X \leq GL(m, p)$, $Y \leq GL(n, p)$, and p does not divide the order of X. Let V be a faithful irreducible KX-module, where $K = GF(p)$. Then the above definition gives that $Y \prec X$ if there exists $X_0 \leq X$ such that $X_0/\ker V_i \cong Y$ for some irreducible KX_0-module V_i, $1 \leq i \leq r$, in the decomposition $V_{X_0} = V_1 \oplus \ldots \oplus V_r$ into irreducible KX_0-modules.

Let $\underline{\underline{X}}$ be a class of (isomorphism classes) of irreducible linear groups over $GF(p)$. We say that $\underline{\underline{X}}$ is *closed* if it contains every irreducible linear factor of every linear group in $\underline{\underline{X}}$. It is clear that the (set-theoretic) union and intersection of closed classes of irreducible linear groups are again closed. In this section, $\underline{\underline{X}}$, $\underline{\underline{Y}}$ will always denote closed classes of irreducible linear groups.

1.2.1 THEOREM (Higman [14]). *Let* $\underline{\underline{X}}$ *be a closed class of irreducible linear groups over* GF(p) *belonging to* $\underline{\underline{W}}$. *Let*

$$\underline{\underline{U}}(\underline{\underline{X}}) = \{G \in \underline{\underline{A}}_p\underline{\underline{W}} : \text{for every minimal normal } p\text{-subgroup } P \text{ of } G,$$
$$\text{the linear group induced in } P \text{ by } G \text{ belongs to } \underline{\underline{X}}\}.$$

Then the correspondence $\underline{\underline{X}} \leftrightarrow \underline{\underline{U}}(\underline{\underline{X}})$ *is a bijection from the closed classes of irreducible linear groups over* GF(p) *belonging to* $\underline{\underline{W}}$ *onto the subvarieties* $\underline{\underline{V}}$ *satisfying* $\underline{\underline{W}} \leq \underline{\underline{V}} \leq \underline{\underline{A}}_p\underline{\underline{W}}$.

1.2.2 LEMMA. *Let* $\underline{\underline{X}}$, $\underline{\underline{Y}}$ *be closed classes. Then*

$$\underline{\underline{U}}(\underline{\underline{X}} \cap \underline{\underline{Y}}) = \underline{\underline{U}}(\underline{\underline{X}}) \wedge \underline{\underline{U}}(\underline{\underline{Y}}),$$
$$\underline{\underline{U}}(\underline{\underline{X}} \cap \underline{\underline{Y}}) = \underline{\underline{U}}(\underline{\underline{X}}) \vee \underline{\underline{U}}(\underline{\underline{Y}}).$$

If $\underline{\underline{X}} \leq \underline{\underline{Y}}$, *then* $\underline{\underline{U}}(\underline{\underline{X}}) \leq \underline{\underline{U}}(\underline{\underline{Y}})$.

Proof. Since every variety is generated by its finitely generated groups (15.61, Hanna Neumann [20]), it follows that every locally finite variety is generated by its finite groups. To prove that two locally finite varieties are identical, it is therefore sufficient to show that every finite group in one of the two varieties also belong to the other.

Let G be any finite group in $\underline{\underline{U}}(\underline{\underline{X}} \cap \underline{\underline{Y}})$. Then for every minimal normal p-subgroup P of G, the linear group induced in P by G belongs to $\underline{\underline{X}}$ and to $\underline{\underline{Y}}$, and therefore $G \in \underline{\underline{U}}(\underline{\underline{X}}) \wedge \underline{\underline{U}}(\underline{\underline{Y}})$. Conversely, every finite group in $\underline{\underline{U}}(\underline{\underline{X}}) \wedge \underline{\underline{U}}(\underline{\underline{Y}})$ belongs to $\underline{\underline{U}}(\underline{\underline{X}} \cap \underline{\underline{Y}})$.

By 15.83, Hanna Neumann [20], $\underline{\underline{U}}(\underline{\underline{X}}) \vee \underline{\underline{U}}(\underline{\underline{Y}})$ is generated by all the finite groups of $\underline{\underline{U}}(\underline{\underline{X}})$ and $\underline{\underline{U}}(\underline{\underline{Y}})$. Thus to show that $\underline{\underline{U}}(\underline{\underline{X}}) \vee \underline{\underline{U}}(\underline{\underline{Y}}) \leq \underline{\underline{U}}(\underline{\underline{X}} \cup \underline{\underline{Y}})$, it is enough to show that the finite groups of $\underline{\underline{U}}(\underline{\underline{X}})$ and $\underline{\underline{U}}(\underline{\underline{Y}})$ belong to $\underline{\underline{U}}(\underline{\underline{X}} \cup \underline{\underline{Y}})$. This is clearly so. Conversely, every finite group in $\underline{\underline{U}}(\underline{\underline{X}} \cup \underline{\underline{Y}})$ belongs to $\underline{\underline{U}}(\underline{\underline{X}})$ or $\underline{\underline{U}}(\underline{\underline{Y}})$ and hence to $\underline{\underline{U}}(\underline{\underline{X}}) \vee \underline{\underline{U}}(\underline{\underline{Y}})$.

The last observation follows from the fact that if $\underline{\underline{X}} \leq \underline{\underline{Y}}$, then $\underline{\underline{X}} = \underline{\underline{X}} \cap \underline{\underline{Y}}$, and hence $\underline{\underline{U}}(\underline{\underline{X}}) = \underline{\underline{U}}(\underline{\underline{X}}) \wedge \underline{\underline{U}}(\underline{\underline{Y}})$. //

We now consider the question of CREAM for subvarieties of $\underline{\underline{A}}_p\underline{\underline{W}}$ when $\underline{\underline{W}}$ is CREAM, reducing the problem to a more manageable situation - in special cases at least. First we shall need the following lemma.

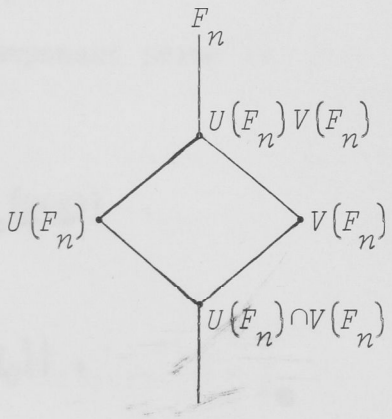
1.2.3 LEMMA. *Suppose that* $\underline{\underline{U}}$ *and* $\underline{\underline{V}}$ *are locally finite*

varieties. Let $f(n)$, $g(n)$, $h(n)$ *and* $k(n)$ *denote the orders of the free groups of rank* n *of* $\underline{\underline{U}}$, $\underline{\underline{V}}$, $\underline{\underline{U}} \wedge \underline{\underline{V}}$ *and* $\underline{\underline{U}} \vee \underline{\underline{V}}$ *respectively. Then*

$$f(n)g(n) = h(n)k(n) .$$

Proof. Let U, V be the closed sets of laws of $\underline{\underline{U}}$, $\underline{\underline{V}}$ respectively. Then the laws of $\underline{\underline{U}} \wedge \underline{\underline{V}}$, $\underline{\underline{U}} \vee \underline{\underline{V}}$ are UV, $U \cap V$ respectively. We have

$$\begin{aligned} f(n)g(n) &= |F_n/U(F_n)| . |F_n/V(F_n)| \\ &= |F_n/(UV)(F_n)| . |(UV)(F_n)/U(F_n)| . \\ &\quad |F_n/(U\cap V)(F_n)| . |V(F_n)/(U\cap V)(F_n)|^{-1} \\ &= h(n)k(n) , \end{aligned}$$



since

$$(UV)(F_n)/U(F_n) = U(F_n)V(F_n)/U(F_n)$$
$$\cong V(F_n)/U(F_n)\cap V(F_n) = V(F_n)/(U\cap V)(F_n) . \qquad //$$

We can then give the following general comment.

1.2.4 THEOREM. *Let* $\underline{\underline{X}}$ *be the class of all irreducible linear groups over* GF(p) *which, as groups, belong to some subvariety* $\underline{\underline{W}}_0 \leq \underline{\underline{W}}$. *Then* $\underline{\underline{U}}(\underline{\underline{X}})$ *is* CREAM *if* $\underline{\underline{W}}_0$ *is* CREAM .

Proof. $\underline{\underline{X}}$ is evidently closed. We claim that $\underline{\underline{U}}(\underline{\underline{X}}) = \underline{\underline{W}} \vee \underline{\underline{A}}_p\underline{\underline{W}}_0$. First we show that $\underline{\underline{U}}(\underline{\underline{X}}) \leq \underline{\underline{W}} \vee \underline{\underline{A}}_p\underline{\underline{W}}_0$. Since a locally finite variety is generated by its critical groups (51.41, Hanna Neumann [20]), it is enough to show that the critical groups in $\underline{\underline{U}}(\underline{\underline{X}})$ belong to $\underline{\underline{W}} \vee \underline{\underline{A}}_p\underline{\underline{W}}_0$. Suppose that G is a critical group in $\underline{\underline{U}}(\underline{\underline{X}})$. For some $G \lhd N \in \underline{\underline{A}}_p$, $G/N \in \underline{\underline{W}}$. N becomes a $K(G/N)$-module, where $K = \mathrm{GF}(p)$, by the action of conjugation, and is completely reducible $p \nmid |G/N|$. Since a critical group is monolithic (51.32, Hanna Neumann [20]), N is irreducible. Thus, by assumption, the linear group induced in N by G belongs to $\underline{\underline{X}}$ and hence to $\underline{\underline{W}}_0$. Since G is monolithic, it follows that N is faithful, and the induced linear group is, in fact, isomorphic to G/N . Hence $G \in \underline{\underline{A}}_p\underline{\underline{W}}_0$. Next we prove the opposite inclusion. Every finite group in $\underline{\underline{W}}$ has

trivial minimal normal p-subgroup and hence induced the trivial linear group, and so belongs to $\underline{\underline{U}}(\underline{\underline{X}})$. Furthermore, suppose that G is a critical group in $\underline{\underline{A}}_p\underline{\underline{W}}_0$. Then, as in the above argument, G has a (unique) minimal normal p-subgroup N such that $G/N \in \underline{\underline{W}}_0$, and the induced linear group is isomorphic to G/N . Therefore $G \in \underline{\underline{U}}(\underline{\underline{X}})$ and so $\underline{\underline{A}}_p\underline{\underline{W}}_0 \leq \underline{\underline{U}}(\underline{\underline{X}})$. Hence $\underline{\underline{W}} \vee \underline{\underline{A}}_p\underline{\underline{W}}_0 \leq \underline{\underline{U}}(\underline{\underline{X}})$.

Moreover $\underline{\underline{W}} \wedge \underline{\underline{A}}_p\underline{\underline{W}}_0 = \underline{\underline{W}}_0$ since $\underline{\underline{W}}$ has exponent prime to p . Thus by Lemma 1.2.3, for all $n \in N^+$,

$$|F_n(\underline{\underline{W}})| . |F_n(\underline{\underline{A}}_p\underline{\underline{W}}_0)| = |F_n(\underline{\underline{W}}_0)| . |F_n(\underline{\underline{U}}(\underline{\underline{X}}))| .$$

As in the proof of Theorem 1.1.4, we have

$$|F_n(\underline{\underline{A}}_p\underline{\underline{W}}_0)| = |F_m(\underline{\underline{A}}_p)| . |F_n(\underline{\underline{W}}_0)| ,$$

where $m = (n-1)|F_n(\underline{\underline{W}}_0)| + 1$. Hence

$$|F_n(\underline{\underline{U}}(\underline{\underline{X}}))| = |F_n(\underline{\underline{W}})| . |F_m(\underline{\underline{A}}_p)| .$$

As we saw in the proof of Theorem 1.1.4, $n \mapsto m$ is the restriction of a CREAM function and so is $n \mapsto |F_m(\underline{\underline{A}}_p)| = p^m$. It follows that $\underline{\underline{U}}(\underline{\underline{X}})$ is CREAM . //

We will need some more facts and lemmas.

1.2.5 LEMMA. *Let* $\underline{\underline{U}}$, $\underline{\underline{V}}$ *and* $\underline{\underline{W}}$ *be varieties satisfying* $\underline{\underline{W}} \leq \underline{\underline{U}} \leq \underline{\underline{V}}\,\underline{\underline{W}}$. *Then* $F_n(\underline{\underline{U}})$ *is an extension of a* $\underline{\underline{V}}$*-group by* $F_n(\underline{\underline{W}})$.

Proof. Let U, V, W be the closed sets of laws of $\underline{\underline{U}}$, $\underline{\underline{V}}$, $\underline{\underline{W}}$ respectively. Then by 14.32, Hanna Neumann [20], we have $W \supseteq U \supseteq V(W)$, and hence

$$W(F_n) \geq U(F_n) \geq (V(W))(F_n) = V(W(F_n)) .$$

$$F_n(\underline{\underline{W}}) = F_n/W(F_n) \cong (F_n/U(F_n))/(W(F_n)/U(F_n)) .$$

But

$$V(W(F_n)/U(F_n)) = V(W(F_n))U(F_n)/U(F_n) = 1 ,$$

and hence (14.22, Hanna Neumann [20]), $W(F_n)/U(F_n) \in \underline{\underline{V}}$. //

1.2.6 LEMMA. *Suppose that* $\underline{\underline{W}} \leq \underline{\underline{U}} \leq \underline{\underline{A}}_p\underline{\underline{W}}$. *Then*

(i) $F_n(\underline{\underline{A}}\ \underline{\underline{W}}_p) = AG_n$,

where $A < F_n(\underline{\underline{A}}\ \underline{\underline{W}}_p)$, $A \in \underline{\underline{A}}_p$, $G_n \cong F_n(\underline{\underline{W}})$;

(ii) $F_n(\underline{\underline{U}}) \cong AG_n/B$,

where $B \lhd AG_n$, $B \leq A$, *and* B *is minimal with respect to the property* $AG_n/B \in \underline{\underline{U}}$.

Proof. *(i)* By Lemma 1.2.5, $F_n(\underline{\underline{A}}\ \underline{\underline{W}}_p)$ is an extension of a group $A \in \underline{\underline{A}}_p$ by $F_n(\underline{\underline{W}})$. By Zassenhaus' Theorem (18.1, Chapter 1, Huppert [16]), $F_n(\underline{\underline{A}}\ \underline{\underline{W}}_p) = AG_n$ where $A \lhd AG_n$, $A \cap G_n = 1$, and so $G_n \cong F_n(\underline{\underline{W}})$.

(ii) Again by Lemma 1.2.5, $F_n(\underline{\underline{U}}) \cong CG_n$ for some $C \in \underline{\underline{A}}_p$. But (14.23, Hanna Neumann [20]), $F_n(\underline{\underline{U}})$ is isomorphic to a factor of $F_n(\underline{\underline{A}}\ \underline{\underline{W}}_p)$, $F_n(\underline{\underline{U}}) \cong AG_n/B$ where $B \lhd AG_n$. Comparing the order of $F_n(\underline{\underline{U}})$, we have $|A| = |B|.|C|$, and hence $B \leq A$.

Suppose that $D \lhd AG_n$, $D < B$ and $AG_n/D \in \underline{\underline{U}}$. Thus AG_n/D is a factor of $F_n(\underline{\underline{U}})$ and hence $|D| \geq |B|$, a contradiction. Therefore B is minimal with respect to the given property. //

1.2.7 LEMMA. *Let* $G_n = F_n(\underline{\underline{W}})$ *and* $K = \mathrm{GF}(p)$. *Then* $F_n(\underline{\underline{A}}\ \underline{\underline{W}}_p) = AG_n$ *where* $A \lhd AG_n$, $A \in \underline{\underline{A}}_p$. *As a* KG_n*-module,* $A = A_1 \oplus \ldots \oplus A_r$, *where the* A_i *are irreducible* KG_n*-modules.*

Let $\underline{\underline{X}}$ be a non-empty closed class, and write $\underline{\underline{U}} = \underline{\underline{U}}(\underline{\underline{X}})$. Then $F_n(\underline{\underline{U}}) \cong AG_n/B$ where $B \lhd AG_n$, $B \leq A$, and as a KG_n-module, $B = A_{i_1} \oplus \ldots \oplus A_{i_s}$ for some $1 \leq i_1 < \ldots < i_s \leq r$, where the irreducible linear group induced by G_n in A_i belongs to $\underline{\underline{X}}$ or does not belong to $\underline{\underline{X}}$ according as $i \neq i_j$, $j = 1, \ldots, s$, or $i = i_j$ for some $1 \leq j \leq s$.

Proof. The first part follows from Lemma 1.2.6. Now A becomes a KG_n-module by the conjugating action of G_n . Since p is prime

to $|G_n|$, we have, by Maschke's Theorem (15.6, Curtis and Reiner [6]),

$$A = A_1 \oplus \ldots \oplus A_r ,$$

where the A_i are irreducible KG_n-modules.

Choose B as in Lemma 1.2.6 *(ii)*. Since A_i is irreducible, $A_i \cap B = 0$ or A_i . If the linear group induced in A_i is not in $\underline{\underline{X}}$, then $A_i \cap B = 0$ is impossible since $AG_n/B \in \underline{\underline{U}}$, and therefore $\underline{\underline{A}}_i \leq B$. Write D for the product of all such A_i so that $D \leq B$. Let C be the product of the remaining A_i . Thus $A = CD$. By definition, $CG_n \in \underline{\underline{U}}$ so that $AG_n/D \in \underline{\underline{U}}$. Hence $D = B$ by the minimality of B . //

Let X be an irreducible linear group over $K = \mathrm{GF}(p)$. We define $c_X(n)$ to be the sum of the K-dimensions of the components in some unrefinable decomposition of the regular representation of G_n over K which are isomorphic, as linear groups, to X . For any non-empty (not necessarily closed) class of irreducible linear groups $\underline{\underline{S}}$, we define $c_{\underline{\underline{S}}}(n) = \sum_{X \in \underline{\underline{S}}} c_X(n)$.

1.2.8 LEMMA. *Let $\underline{\underline{X}}$ be a non-empty closed class. Then*

$$|F_n(\underline{\underline{U}}(\underline{\underline{X}}))| = |F_n(\underline{\underline{W}})| . p^{1+(n-1)c_{\underline{\underline{X}}}(n)} .$$

Proof. By Lemma 1.2.7, $|F_n(\underline{\underline{U}}(\underline{\underline{X}}))| = |A/B| . |G_n|$. Moreover $|A/B| = p^m$ where m is the sum of the K-dimensions of the components in an unrefinable direct decomposition of A which belong as linear groups to $\underline{\underline{X}}$. However, by a theorem of Gaschütz [7], A is the direct sum of the trivial representation and $n - 1$ copies of the regular representation of G_n . Hence $m = 1 + (n-1)c_{\underline{\underline{X}}}(n)$. //

Let X be an irreducible linear group and G a finite group. An epimorphism of G onto X determines a representation of G . We say that two epimorphisms of G onto X are *equivalent* if they are equivalent as representations; otherwise we say they are *inequivalent*.

1.2.9 LEMMA. *Let G be a finite group and X an irreducible linear group over K. The number of inequivalent irreducible representations of G whose induced linear group is isomorphic to X is equal to the number of inequivalent epimorphisms of G onto X.*

Proof. Let ρ be an irreducible representation of G whose induced linear group is isomorphic to $X \leq \mathrm{GL}(r, K)$,

$$\rho : G \twoheadrightarrow Y \leq \mathrm{GL}(r, K)$$

where $X \tilde{=} Y$. From the introductory remarks in this section, we have $Y = u^{-1}Yu$ for some $u \in \mathrm{GL}(r, K)$. Define the following epimorphism $\varepsilon : G \twoheadrightarrow X$ by $g\varepsilon = u(g\rho)u^{-1}$. Then $\rho = \varepsilon\varphi_u$ where φ_u is the inner automorphism of $\mathrm{GL}(r, K)$ induced by u. Conversely, for every epimorphism ε of G onto X and every $u \in \mathrm{GL}(r, K)$, $\rho = \varepsilon\varphi_u$ gives a representation of G with the induced linear group isomorphic to X.

Let $\sigma = \delta\varphi_v$ where δ is an epimorphism of G onto X and $v \in \mathrm{GL}(r, K)$. It is then clear that ρ is equivalent to σ if and only if ε is equivalent to δ. //

We recall two definitions. Let X be an irreducible linear group over K so that $X \leq \mathrm{GL}(r, K)$ for some r. We call an automorphism α of X a *linear automorphism* if there exists $u \in \mathrm{GL}(r, K)$ such that $x\alpha = u^{-1}xu$ for all $x \in X$. We denote by lin aut X the group of all linear automorphisms of X.

The *Eulerian function* k_G of a group G is a function $N^+ \to N^+ \cup \{0\}$ given by: $k_G(n)$ is the number of order n-tuples $(g_1, \ldots, g_n)$ which generate G.

1.2.10 LEMMA. *Let $G_n = F_n(\underline{\underline{W}})$ and X an irreducible linear group which belongs, as an abstract group, to $\underline{\underline{W}}$. Then the number of inequivalent irreducible representations of G_n in which the induced linear group is isomorphic to X is equal to $k_X(n)/|\text{lin aut } X|$.*

Proof. It is sufficient, by Lemma 1.2.9, to enumerate the number of inequivalent epimorphisms of G_n onto X. Suppose that ρ and σ are two epimorphisms of G_n onto X. We claim that ρ is

equivalent to σ if and only if $\rho = \sigma\alpha$ for some $\alpha \in \text{lin aut } X$. With the notations in the proof of Lemma 1.2.9, ρ equivalent to σ implies that $\rho = \sigma\varphi_u$ for some $u \in GL(r, K)$. Note that X admits φ_u and hence $\varphi_u|_X \in \text{lin aut } X$. Conversely, if $\rho = \sigma\alpha$ for some $\alpha \in \text{lin aut } X$, then for every $g \in G_n$, $g\rho = u^{-1}(g\sigma)u$ for some $u \in GL(r, K)$, so that ρ is equivalent to σ.

In this way, the epimorphisms of G_n onto X fall into equivalence classes. Let ρ belong to some equivalence class. Then every member of this class is of the form $\rho\alpha$ for some $\alpha \in \text{lin aut } X$. It is clear that for all $\alpha_1, \alpha_2 \in \text{lin aut } X$, $\alpha_1 \neq \alpha_2$ if and only if $\rho\alpha_1 \neq \rho\alpha_2$. Hence each equivalence class contains exactly $|\text{lin aut } X|$ elements.

Next, fix a set of generators $\{g_1, \ldots, g_n\}$ for G_n. We note that a mapping of $\{g_1, \ldots, g_n\}$ into X can be extended to a homomorphism. For the laws of G_n are precisely those of $\underline{\underline{W}}$, and so every identical relation $w(g_1, \ldots, g_n) = 1$ in G_n remains a valid relation $w(g_1\theta, \ldots, g_n\theta) = w(g_1, \ldots, g_n)\theta = 1$ under the mapping θ of $\{g_1, \ldots, g_n\}$ into X since $X \in \underline{\underline{W}}$. Consequently, by von Dyck's Theorem (Corollary to Theorem 21, B.H. Neumann [19]), θ may be extended uniquely to a homomorphism. In other words, a homomorphism of G_n into X is completely specified by its images on the generators $\{g_1, \ldots, g_n\}$, and therefore the total number of epimorphisms of G_n onto X is just $k_X(n)$. Thus there are $k_X(n)/|\text{lin aut } X|$ distinct equivalence classes. //

We are now in a position to give an explicit expression for $c_X(n)$.

1.2.11 LEMMA. *Let X be an irreducible linear group over $K = GF(p)$, and M the irreducible module on which X acts. Then*

$$c_X(n) = \frac{(\dim_K M)^2 k_X(n)}{(\dim_K \text{End}_{KX} M)\,|\text{lin aut } X|}.$$

Proof. Fix some unrefinable direct decomposition of the regular

representation of G_n over K. Let M be an irreducible component in this decomposition which is isomorphic as a linear group to X. M is a faithful irreducible KX-module and $G_n/\ker M \tilde{=} X$ where $\ker M$ is the kernel of M as a KG_n-module. From §§ 25, 26 of Curtis and Reiner [6], the number of times M occurs in this decomposition is equal to the dimension of M over $\mathrm{End}_{KG_n} M$, or $\dim_K M/\dim_K \mathrm{End}_{KX} M$, since $\mathrm{End}_{KG_n} M = \mathrm{End}_{KX} M$. Since every irreducible representation of G_n occurs in the regular representation of G_n, the required expression for $c_X(n)$ then follows from Lemma 1.2.10. //

Hall [10] has shown that for any finite group G, $k_G(n)$ is of the form $k_G(n) = \sum_{H \leq G} m_H |H|^n$, where the m_H are integers independent of n, and hence $k_G : N^+ \to \mathbb{R}$ so defined is evidently the restriction of a CREAM function. So also is the function c_X for an irreducible linear group X. Together with Lemma 1.2.8, this gives the following theorem.

1.2.12 THEOREM. *If $\underline{\underline{X}}$ is a non-empty finite closed class, then $\underline{\underline{U}}(\underline{\underline{X}})$ is* CREAM.

As a consequence of the above remarks and Theorem 1.2.4, we have

1.2.13 LEMMA. *If $\underline{\underline{X}}$ is the union of the set of irreducible linear groups in a* CREAM *subvariety and a finite set, then $\underline{\underline{U}}(\underline{\underline{X}})$ is* CREAM.

Together with Lemma 1.2.8, the Higman correspondence $\underline{\underline{X}} \leftrightarrow \underline{\underline{U}}(\underline{\underline{X}})$ reduces the CREAM problem for the subvarieties of $\underline{\underline{A}}_p\underline{\underline{W}}$ containing $\underline{\underline{W}}$, when $\underline{\underline{W}}$ is CREAM, to one concerned entirely with the closed classes $\underline{\underline{X}}$ of irreducible linear groups, namely:

Is the function $n \mapsto c_{\underline{\underline{X}}}(n)$ the restriction of a CREAM *function?*

1.3 The case when $\underline{\underline{W}}$ is a direct join

This section is essentially a follow-up of the ideas and methods

developed in the preceding section. Here we consider the case when $\underline{\underline{W}} = \underline{\underline{W}}_1 \vee \underline{\underline{W}}_2$ where the exponents of $\underline{\underline{W}}_1$ and $\underline{\underline{W}}_2$ are coprime. Moreover we assume that $c_{\underline{\underline{X}}_i}$ is the restriction of a CREAM function for all closed classes $\underline{\underline{X}}_i \subseteq \underline{\underline{W}}_i$, $i = 1, 2$, so that the subvarieties between $\underline{\underline{W}}_i$ and $\underline{\underline{A}}_p\underline{\underline{W}}_i$, $i = 1, 2$, are CREAM. We shall see that under certain conditions, the subvarieties between $\underline{\underline{W}}$ and $\underline{\underline{A}}_p\underline{\underline{W}}$ would be CREAM.

We use the terminology in the preceding section. We write G_n, G_{1n}, G_{2n} for the free groups of rank n of $\underline{\underline{W}}$, $\underline{\underline{W}}_1$, $\underline{\underline{W}}_2$ respectively, and $\underline{\underline{X}}_i$, $i = 1, 2$, will always denote closed classes of irreducible linear groups over $K = \mathrm{GF}(p)$ in $\underline{\underline{W}}_i$. First an elementary observation.

1.3.1 LEMMA. *A finite group in* $\underline{\underline{W}}$ *is a direct product of a group in* $\underline{\underline{W}}_1$ *and a group in* $\underline{\underline{W}}_2$.

Proof. By 21.33, Hanna Neumann [20], $G_n = G_{1n} \times G_{2n}$. Every finite group in $\underline{\underline{W}}$ is a factor of G_n for some $n \in N^+$. But a subgroup H of $G_{1n} \times G_{2n}$ is of the form $H = H_1 \times H_2$ where $H_i = H \cap G_{in}$, $i = 1, 2$, since the exponents of G_{1n}, G_{2n} are coprime. Hence a group in $\underline{\underline{W}}$ is isomorphic to $G_{1n} \times G_{2n}/H \cong G_{1n}/H_1 \times G_{2n}/H_2$. //

Let X be an irreducible linear group in $\underline{\underline{W}}$. Then the above lemma tells us that $X = X_1 \times X_2$, or simply $X = X_1X_2$, where $X_i \in \underline{\underline{W}}_i$, $i = 1, 2$. Obviously X determines X_1 and X_2 as abstract groups. In fact, we have more.

1.3.2 LEMMA. X_i *is an irreducible linear group uniquely determined by* X *for* $i = 1, 2$.

Proof. Let M be a faithful irreducible KX-module. Since X_1 is a direct factor of X, we have, by Clifford's Theorem (49.2, Curtis and Reiner [6]),

$$M_{X_1} = M_1 \oplus \ldots \oplus M_r ,$$

where the M_i are isomorphic irreducible KX_1-modules and hence each M_i is faithful. In particular, the M_i are all linearly isomorphic.

Suppose that N is a faithful irreducible KX-module linearly isomorphic to M. As in above, we have

$$N_{X_1} = N_1 \oplus \ldots \oplus N_r ,$$

where the N_i are isomorphic faithful irreducible KX_1-modules. We show that the M_i and N_j are isomorphic KX_1-modules. First there is a bijective linear transformation $\gamma : M \to N$ such that $\gamma^{-1} X \gamma = X$. Then $N_{X_1} = M\gamma = M_1\gamma \oplus \ldots \oplus M_r\gamma$, where it is easily seen that the $M_i\gamma$ are irreducible KX_1-modules if the action of X_1 on $M_i\gamma$ is given by $u \circ x_1 = u\left(\gamma^{-1} x_1 \gamma\right)$. Thus

$$N_1 \oplus \ldots \oplus N_r = M_1\gamma \oplus \ldots \oplus M_r\gamma .$$

It follows from the Krull-Schmidt Theorem (14.5, Curtis and Reiner [6]) that, with suitable re-indexing, $N_i \cong M_i\gamma$, $i = 1, \ldots, r$. Moreover, as modules, $M_i \cong M_i\gamma$ and so $M_i \cong N_i$. //

1.3.3 LEMMA. *If* $Y_1 Y_2 = Y \prec X = X_1 X_2$, *then* $Y_1 \prec X_1$, $Y_2 \prec X_2$.

Proof. Let M be a faithful irreducible KX-module. Then there exists $X_0 \leq M$ such that $M_{X_0} = M_1 \oplus \ldots \oplus M_r$ and $X_0/\ker M_1 = Y$, where the M_i are irreducible KX_0-modules. As remarked in the proof of Lemma 1.3.1, $X_0 = X_{01} X_{02}$ where $X_{0i} \leq X_i$, $i = 1, 2$. By Clifford's Theorem,

$$(M_1)_{X_{0i}} = M_{i1} \oplus \ldots \oplus M_{is_i} , \quad i = 1, 2 ,$$

where the M_{ij} are isomorphic irreducible KX_{0i}-modules, and hence $\ker M_{ij} = \ker M_1 \cap X_{0i}$, $j = 1, \ldots, s_i$. But

$$\ker M_1 = (\ker M_1 \cap X_{01}).(\ker M_1 \cap X_{02}) = \ker M_{11}.\ker M_{21} .$$

Hence $X_0/\ker M_1 \cong X_{01}/\ker M_{11}.X_{02}/\ker M_{21}$. Since $X_{0i}/\ker M_{i1}$, $i = 1, 2$, are uniquely determined irreducible linear groups, it follows that $X_{0i}/\ker M_{i1}$ is isomorphic, as linear group, to Y_i , $i = 1, 2$. //

For non-empty closed classes $\underline{\underline{X}}_i$, $i = 1, 2$, we define the class $\underline{\underline{X}}_1 \otimes \underline{\underline{X}}_2$ as the class of all irreducible linear groups $X = X_1X_2$ in $\underline{\underline{W}}$ such that $X_i \in \underline{\underline{X}}_i$, $i = 1, 2$. That is, if M is a faithful irreducible KX-module so that $M_{X_i} \cong M_i \oplus \ldots \oplus M_i$ where M_i is a faithful irreducible KX_i-module for $i = 1, 2$, then the irreducible linear group X_i induced from M_i belongs to $\underline{\underline{X}}_i$, $i = 1, 2$. Evidently $\underline{\underline{X}}_1 \otimes \underline{\underline{X}}_2$ is closed.

1.3.4 THEOREM. $c_{\underline{\underline{X}}_1 \otimes \underline{\underline{X}}_2}(n) = c_{\underline{\underline{X}}_1}(n).c_{\underline{\underline{X}}_2}(n)$.

Proof. Let R_i be the regular KG_{in}-module, $i = 1, 2$, and let $R_i = M_i \oplus N_i$ where M_i is the sum of all the irreducible components in some fixed unrefinable direct decomposition of R_i which belong as linear groups to $\underline{\underline{X}}_i$ for $i = 1, 2$. It is clear that $R = R_1 \# R_2$ is the regular KG_n-module, and that $R \cong M \oplus N$, where $M = M_1 \# M_2$, $N = (M_1 \# N_2) \oplus (N_1 \# M_2) \oplus (N_1 \# N_2)$.

We show that an irreducible component in M induces a linear group in $\underline{\underline{X}}_1 \otimes \underline{\underline{X}}_2$. Let M_0 be any irreducible KG_n-submodule of M . M_0 determines an irreducible linear group $X = X_1X_2$. Since $M_{G_{in}}$ is a direct sum of copies of M_i , it follows that $(M_0)_{G_{in}}$ is a direct sum of copies of an irreducible component of M_i . But $(M_0)_{G_{in}}$ induces an irreducible linear group isomorphic to X_i . Hence by the definition of M_i , $X_i \in \underline{\underline{X}}_i$, and so $X \in \underline{\underline{X}}_1 \otimes \underline{\underline{X}}_2$.

Next we show that an irreducible component in N cannot induce a linear group in $\underline{\underline{X}}_1 \otimes \underline{\underline{X}}_2$. Let N_0 be any irreducible KG_n-submodule

of N . We may assume that N_0 is a KG_n-submodule of $M_1 \# M_2$. N_0 determines an irreducible linear group $Y = Y_1 Y_2$. As in above, $(N_0)_{G_{2n}}$ is a direct sum of copies of an irreducible component of N_2 , and so the induced irreducible linear group Y_2 is not in $\underline{\underline{X}}_2$ by the definition of M_2 . Hence $Y \notin \underline{\underline{X}}_1 \otimes \underline{\underline{X}}_2$.

Thus we have

$$c_{\underline{\underline{X}}_1 \otimes \underline{\underline{X}}_2}(n) = \dim_K M = (\dim_K M_1).(\dim_K M_2) = c_{\underline{\underline{X}}_1}(n) c_{\underline{\underline{X}}_2}(n) . \qquad //$$

Clearly, if $\underline{\underline{U}}(\underline{\underline{X}}_i)$, $i = 1, 2$, are CREAM , then so is $\underline{\underline{U}}(\underline{\underline{X}}_1 \otimes \underline{\underline{X}}_2)$. Unfortunately it may not be possible to build up the closed classes in $\underline{\underline{W}}$ from the classes $\underline{\underline{X}}_1 \otimes \underline{\underline{X}}_2$. In fact, though X determines the irreducible linear groups $X_1 X_2$, the converse is not true. If, however, X_1, X_2 satisfy the following condition, called *Condition* H , then we shall show that they do determine X .

Condition H : The tensor product $X_1 \otimes X_2$ over K is a direct sum of isomorphic irreducible linear groups; or in terms of modules, if M_i is the faithful irreducible KX_i-module, $i = 1, 2$, then $M_1 \# M_2$ is a direct sum of linearly isomorphic faithful irreducible KX-modules.

We shall need the following theorem.

1.3.5 THEOREM (Brady, Bryce and Cossey [4]). *Let X be a finite group, E a field, E^* the algebraic closure of E , and T_1, T_2 faithful irreducible representations of X over E . Then T_1, T_2 are linearly isomorphic if and only if some composition factor $T_1^{E^*}$ is linearly isomorphic to a composition factor of $T_2^{E^*}$.*

1.3.6 LEMMA. *Let X_1, X_2 be irreducible linear groups satisfying condition* H. *Then X_1, X_2 determine X uniquely.*

Proof. Let M_i be faithful irreducible KX_i-modules, $i = 1, 2$, so that $M_1 \# M_2 \cong M_1' \oplus \ldots \oplus M_r'$, where the M_j' are linearly

isomorphic faithful irreducible KX-modules, $X = X_1X_2$. Suppose that N is another faithful irreducible KX-module so that $N_{X_i} \cong N_i \oplus \ldots \oplus N_i$ where N_i is a faithful irreducible KX_i-module for $i = 1, 2$. We have to prove that if N_i is linearly isomorphic to M_i, $i = 1, 2$, then N is linearly isomorphic to M'_j, $1 \leq j \leq r$.

First we note that (6.15, Chapter 3, Gorenstein [9]) every irreducible representation of X over the algebraic closure K^* of K can be written in some finite extension field F' of K such that F' is splitting for X. Moreover, there is an extension F of F' that is a finite normal extension of K (49.5.1, Warner [25]) and hence also splitting for X. Thus by 70.15, Curtis and Reiner [6],

$$N^F = L_1 \oplus \ldots \oplus L_s ,$$

where each L_i is a faithful irreducible FX-module. Now

$$(N^F)_{X_i} = \left(N_{X_i}\right)^F \cong \left(N_{i1} \oplus \ldots \oplus N_{it_i}\right) \oplus \ldots \oplus \left(N_{i1} \oplus \ldots \oplus N_{it_i}\right)$$

where $N_i^F = N_{i1} \oplus \ldots \oplus N_{it_i}$, and each N_{ij} is a faithful irreducible FX_i-module for $i = 1, 2$. It follows that $(L_1)_{X_i}$ has an irreducible FX_i-submodule $L_{1i} \cong N_{ik_i}$ for some $1 \leq k_i \leq t_i$. Hence by 2.7, Brady, Bryce and Cossey [4],

$$L_1 \cong L_{11} \# L_{12} \cong N_{1k_1} \# N_{2k_2} .$$

Since M_i is linearly isomorphic to N_i, we have

$$M_i^F = M_{i1} \oplus \ldots \oplus M_{it_i} , \quad i = 1, 2 ,$$

where M_{ij} is linearly isomorphic to N_{ij}, $j = 1, \ldots, t_i$. Thus L_1 is linearly isomorphic to $M_{1k_1} \# M_{2k_2}$. Moreover,

$$M_1'^F \oplus \ldots \oplus M_r'^F = M_1^F \# M_2^F = \bigoplus_{j=1}^{t_1} \bigoplus_{k=1}^{t_2} M_{1j} \# M_{2k} ,$$

where each $M_{1j} \# M_{2k}$ is a faithful irreducible FX-module. It follows that L_1 is linearly isomorphic to some composition factor fo $M_j'^F$, $1 \le j \le r$, and hence by Theorem 1.3.5, N is linearly isomorphic to M_j'. //

Condition H is indeed satisfied if K is a splitting field for X_1 or X_2. It is well-known that $K = \mathrm{GF}(p)$ is splitting for X_i if $p \equiv 1 \pmod{m_i}$ where m_i is the exponent of X_i. In fact, a well-known result in number theory called Dirichlet's Theorem (Hardy and Wright [12]) tells us that there are infinitely many primes of the form. Yet another sufficient condition for Condition H to be satisfied is the following.

1.3.7 LEMMA. *Suppose that X_i has only one linear isomorphism class over the algebraic closure K^* of K for $i = 1, 2$. Then X_1, X_2 satisfy Condition* H.

Proof. Let M_i be a faithful irreducible KX_i-module, $i = 1, 2$. Since the irreducible representations of X_i over K^* can be written in a finite normal extension field E_i of K that is also splitting for X_i, we may assume that $E = E_1 = E_2$. In fact, we may assume that E is also splitting for $X = X_1X_2$. Suppose that

$$M_i^E = M_{i1} \oplus \ldots \oplus M_{ir_i}, \quad i = 1, 2,$$

where the M_{ij} are linearly isomorphic faithful irreducible EX_i-modules by assumption. Let

$$M_1 \# M_2 = L_1 \oplus \ldots \oplus L_s,$$

where each L_i is a faithful irreducible KX-module. We wish to show that the L_i are linearly isomorphic. Now

$$L_1^E \oplus \ldots \oplus L_s^E = M_1^E \# M_2^E$$

$$= \bigoplus_{j=1}^{r_1} \bigoplus_{k=1}^{r_2} M_{1j} \# M_{2k},$$

e

where the $M_{1j} \# M_{2k}$ are linearly isomorphic faithful irreducible KX-modules. Hence L_i^E has a composition factor linearly isomorphic to a composition factor of L_j^E for $1 \le i$, $j \le s$. Therefore L_i, L_j are linearly isomorphic by Theorem 1.3.5. //

An important consequence of Condition H is the following.

1.3.8 LEMMA. *Suppose that* X_i, Y_i, $i = 1, 2$, *satisfy Condition* H. *Then*

$$Y \prec X \text{ if and only if } Y_1 \prec X_1, \quad Y_2 \prec X_2.$$

Proof. Necessity is given by Lemma 1.3.3. To prove sufficiency, let M_i be a faithful irreducible KX_i-module, $i = 1, 2$. Then there exists $X_{0i} \le X_i$, $i = 1, 2$, such that

$$(M_i)_{X_{0i}} = M_{i1} \oplus \ldots \oplus M_{ir_i},$$

where M_{i1} is a faithful irreducible KY_i-module, with $Y_i = X_{0i}/\ker M_{i1}$ as abstract groups. By assumption,

$$M_{11} \# M_{21} = L_1 \oplus \ldots \oplus L_s,$$

where the L_i are linearly isomorphic faithful irreducible XY-modules, and $Y = Y_1 Y_2$ as abstract groups. Also

$$M_1 \# M_2 = N_1 \oplus \ldots \oplus N_t,$$

where the N_i are linearly isomorphic faithful irreducible KX-modules, and $X = X_1 X_2$ as abstract groups.

Put $X_0 = X_{01} X_{02}$. Then

$$(N_1)_{X_0} \oplus \ldots \oplus (N_t)_{X_0} \cong (M_1)_{X_{01}} \# (M_2)_{X_{02}}$$

$$\cong \bigoplus_{j=1}^{r_1} \bigoplus_{k=1}^{r_2} M_{1j} \# M_{2k}.$$

Now each L_i may be considered as an irreducible KX_0-module with kernel equal to $\ker M_{11} . \ker M_{21}$. Therefore L_1 is isomorphic to an

irreducible KX_0-submodule N_0 of $(N_i)_{X_0}$ for some $1 \le i \le t$.

Hence L_1, N_0 are isomorphic as KY-modules, that is $Y \prec X$. //

In the rest of this section, we assume that Condition H is satisfied by all linear groups in $\underline{\underline{W}}_i$, $i = 1, 2$. Given any two irreducible linear groups X_1, X_2, we write X_1X_2 for the irreducible linear group uniquely determined by the tensor product $X_1 \otimes X_2$. It is then clear that every irreducible linear group in $\underline{\underline{W}}$ may be uniquely expressed in the form X_1X_2 for some irreducible linear group $X_i \in \underline{\underline{W}}_i$, $i = 1, 2$. The class $\underline{\underline{X}}_1 \otimes \underline{\underline{X}}_2$ is then given by $\underline{\underline{X}}_1 \otimes \underline{\underline{X}}_2 = \{X_1X_2 : X_i \in \underline{\underline{X}}_i, \ i = 1, 2\}$. Indeed every closed class in $\underline{\underline{W}}$ is then determined by such classes in the following way.

1.3.9 THEOREM. *Every closed class $\underline{\underline{X}}$ in $\underline{\underline{W}}$ is the union of the maximal classes of the form $\underline{\underline{X}}_1 \otimes \underline{\underline{X}}_2$ contained in $\underline{\underline{X}}$.*

Proof. Let

$$\underline{\underline{S}} = \cup\{\underline{\underline{Y}} : \underline{\underline{Y}} = \underline{\underline{X}}_1 \otimes \underline{\underline{X}}_2 \text{ and } \underline{\underline{Y}} \text{ is maximal with respect to } \underline{\underline{Y}} \le \underline{\underline{X}}\}.$$

Clearly $\underline{\underline{S}} \le \underline{\underline{X}}$. Suppose that $X_1X_2 \in \underline{\underline{X}}$. Define $\underline{\underline{X}}_i$, $i = 1, 2$, to be the closure of X_i. It is easily checked that the closure of X_1X_2 is $\underline{\underline{X}}_1 \otimes \underline{\underline{X}}_2$ so that $\underline{\underline{X}}_1 \otimes \underline{\underline{X}}_2 \le \underline{\underline{X}}$. Evidently $\underline{\underline{X}}_1 \otimes \underline{\underline{X}}_2$ is contained in some maximal class $\underline{\underline{Y}}$ of $\underline{\underline{S}}$. //

However the union of such maximal classes may be infinite. So we need more hypotheses.

1.3.10 LEMMA. *Suppose that the closed classes $\underline{\underline{X}}_i$ in $\underline{\underline{W}}_i$ satisfy the descending chain condition for $i = 1, 2$. Then every closed class $\underline{\underline{X}}$ in $\underline{\underline{W}}$ is a finite union of maximal classes of the form $\underline{\underline{X}}_1 \otimes \underline{\underline{X}}_2$ contained in $\underline{\underline{X}}$.*

Proof. By Theorem 1.3.9, $\underline{\underline{X}} = \bigcup_{\lambda \in \Lambda} \underline{\underline{X}}_1^{(\lambda)} \otimes \underline{\underline{X}}_2^{(\lambda)}$, where $\underline{\underline{Y}}^{(\lambda)} = \underline{\underline{X}}_1^{(\lambda)} \otimes \underline{\underline{X}}_2^{(\lambda)}$ is maximal with respect to $\underline{\underline{Y}}^{(\lambda)} \le \underline{\underline{X}}$, and Λ is some index set. We want to show that Λ may be chosen finite.

Consider the correspondence $\underline{\underline{X}}_1^{(\lambda)} \leftrightarrow \underline{\underline{X}}_2^{(\lambda)}$, $\lambda \in \Lambda$. It is

clearly onto. We claim that $\underline{\underline{X}}_1^{(\mu)} \leq \underline{\underline{X}}_1^{(\lambda)}$ implies that $\underline{\underline{X}}_2^{(\mu)} \geq \underline{\underline{X}}_2^{(\lambda)}$. For putting $\underline{\underline{X}}_1 = \underline{\underline{X}}_1^{(\mu)}$, $\underline{\underline{X}}_2 = \underline{\underline{X}}_2^{(\lambda)} \cup \underline{\underline{X}}_2^{(\mu)}$, we have

$$\underline{\underline{X}}_1^{(\mu)} \otimes \underline{\underline{X}}_2^{(\mu)} \leq \underline{\underline{X}}_1 \otimes \underline{\underline{X}}_2 \leq \underline{\underline{X}} .$$

By maximality, we have $\underline{\underline{X}}_1 \otimes \underline{\underline{X}}_2 = \underline{\underline{X}} = \underline{\underline{X}}_1^{(\mu)} \otimes \underline{\underline{X}}_2^{(\mu)}$ or $\underline{\underline{X}}_1 \otimes \underline{\underline{X}}_2 = \underline{\underline{X}}_1^{(\mu)} \otimes \underline{\underline{X}}_2^{(\mu)}$. In either case, we have $\underline{\underline{X}}_2^{(\lambda)} \cup \underline{\underline{X}}_2^{(\mu)} = \underline{\underline{X}}_2^{(\mu)}$ so that $\underline{\underline{X}}_2^{(\lambda)} \leq \underline{\underline{X}}_2^{(\mu)}$. It also follows that the above correspondence is one-to-one. Hence if $\underline{\underline{X}}_1^{(\mu)} < \underline{\underline{X}}_1^{(\lambda)}$, then $\underline{\underline{X}}_2^{(\mu)} > \underline{\underline{X}}_2^{(\lambda)}$, all inclusions being strict.

The closed classes $\underline{\underline{X}}_1$ in $\underline{\underline{W}}_1$ are partially well-ordered by inclusion, and hence by 2.1, Higman [*13*], the set $\left\{\underline{\underline{X}}_1^{(\lambda)} : \lambda \in \Lambda\right\}$ has a finite number of minimal elements. Either all the ascending chains in this set are finite in length, in which case Λ is finite, or else there is at least one infinite ascending chain in the set $\underline{\underline{X}}_1^{(1)} < \underline{\underline{X}}_1^{(2)} < \ldots$ say. Then by the preceding remarks, we get an infinite descending chain $\underline{\underline{X}}_2^{(1)} > \underline{\underline{X}}_2^{(2)} > \ldots$, contradicting the assumption that the closed classes in $\underline{\underline{W}}_2$ satisfy the descending chain condition. //

1.3.11 THEOREM. *Suppose that the closed classes* $\underline{\underline{X}}_i$ *in* $\underline{\underline{W}}_i$ *satisfy the descending chain condition for* $i = 1, 2$. *Then the subvarieties of* $\underline{\underline{A}}_p \underline{\underline{W}}$ *containing* $\underline{\underline{W}}$ *are* CREAM.

Proof. By the remarks at the end of Section 1.2, it is sufficient to show that $c_{\underline{\underline{X}}}$ is the restriction of a CREAM function for every closed class $\underline{\underline{X}}$ in $\underline{\underline{W}}$. By Lemma 1.3.10, $\underline{\underline{X}}$ is of the form $\underline{\underline{X}} = \bigcup_{j=1}^{m} \underline{\underline{X}}_1^{(j)} \otimes \underline{\underline{X}}_2^{(j)}$ for some positive integer m and closed classes $\underline{\underline{X}}_i^{(j)}$ in $\underline{\underline{W}}_i$, $i = 1, 2$. From Theorem 1.3.4, we have

$$c_{\underline{\underline{X}}}(n) = \sum_{j=1}^{m} c_{\underline{\underline{X}}_1^{(j)}}(n) \cdot c_{\underline{\underline{X}}_2^{(j)}}(n) .$$

By assumption, each $c_{\underline{\underline{X}}_i^{(j)}}$ is the restriction of a CREAM function, and hence so is $c_{\underline{\underline{X}}}$ by Lemma 1.1.1. //

In subsequent chapters, every irreducible linear group we will be concerned with has only one linear isomorphism class over any field whose characteristic does not divide the order of the linear group. We will see that this enables us to obtain a more workable formula for $c_{\underline{\underline{X}}}(n)$. So suppose that there is only one linear isomorphism class of irreducible linear groups in $\underline{\underline{W}}$ over the algebraic closure K^* of K . Theorem 1.3.5 tells us that there is only one linear isomorphism class of irreducible linear groups in $\underline{\underline{W}}$ over K . Thus every irreducible linear group X over K determines and is uniquely determined by an irreducible linear group X^* over K^* . We define $c_{X^*}(n)$ to be the sum of the K^*-dimensions of the components in some unrefinalbe direct decomposition of the regular representation of G_n over K^* which are isomorphic, as linear groups, to X^* . Under these conditions we have:

1.3.12 THEOREM. $c_X(n) = c_{X^*}(n)$.

Proof. Let M be the regular KG_n-module. Suppose that

$$M = M_1 \oplus \ldots \oplus M_r ,$$

where each M_i is an irreducible KG_n-module and hence a faithful irreducible KX_i-module, writing $X_i = G_n/\ker M_i$ as abstract groups.

The irreducible representations of G_n over K^* may be written in some finite normal extension field F of K which is a splitting field for G_n . Hence by 70.15, Curtis and Reiner [6],

$$M_i^F = M_{i1} \oplus \ldots \oplus M_{is_i} , \quad i = 1, \ldots, r ,$$

where the M_{ij} are linearly isomorphic faithful irreducible FX_i-modules. The regular FG_n-module is then

$$M^F = \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{s_i} M_{ij} .$$

Suppose that N is a faithful irreducible FX-module so that

$$N^F = N_1 \oplus \ldots \oplus N_t ,$$

where the N_i are linearly isomorphic faithful irreducible LX-modules. Then, by Theorem 1.3.5, N is linearly isomorphic to M_i if and only if $X \tilde{=} X_i$ as abstract groups and N_1 is linearly isomorphic to M_{ij}, $j = 1, \ldots, s_i$. Let I be the index set such that N is linearly isomorphic to M_i if and only if $i \in I$. Then

$$\begin{aligned} c_X(n) &= \sum_{i \in I} \dim_K M_i \\ &= \sum_{i \in I} \sum_{j=1}^{s_i} \dim_F M_{ij} \\ &= c_{X^*}(n) , \end{aligned}$$

where X^* is the linear group over K^* corresponding to the linear group X over K. //

1.3.13 COROLLARY. $c_X(n) = \left(\dim_{K^*} M^*\right)^2 k_X(n) / |\text{lin aut } X^*|$, *where* M^* *is the module over* K^* *on which* X^* *acts.*

Proof. By Schur's Lemma (5.3, Chapter 3, Gorenstein [9]), $\text{End}_{K^*X^*} M^* = K^*$, and the corollary follows from Lemmas 1.3.12 and 1.2.11. //

CHAPTER 2

FINITE q-GROUPS OF CLASS TWO WITH CYCLIC CENTRE

2.1 Preliminaries

We recall the definition of a central product (see, for example, B.H. Neumann [19]). Let A, B be any two groups, and let $H \leq Z(A)$, $K \leq Z(B)$ and θ an isomorphism of H onto K. Put $N = \{(h^{-1}, h\theta) : h \in H\}$ which is easily seen to be normal in $A \times B$. Then the factor group $G = A \times B/N$ is called the *central product* of A and B (with respect to H and θ). If we identify H with K Under the isomorphism θ, we can alternatively say that G is a central product of A and B with amalgamated subgroup H if $G = AB$ where $A \cap B = H$, and every element of A commutes with every element of B.

In general, the central product of A and B depends on the amalgamation θ. Under suitable conditions, two central products of A and B could be isomorphic.

2.1.1 THEOREM. *Let A, B be groups, $H \leq Z(A)$, $K \leq Z(B)$, and let θ, φ be isomorphisms of H onto K. If $\theta\varphi^{-1}$ can be extended to an automorphism of A, then the central products of A and B with respect to the amalgamations θ and φ are isomorphic.*

Proof. Let

$$M = \{(h^{-1}, h\theta) : h \in H\},$$

$$N = \{(h^{-1}, h\varphi) : h \in H\}.$$

Suppose that $\theta\varphi^{-1}$ can be extended to some $\alpha \in \text{aut } A$ so that $\alpha|_H = \theta\varphi^{-1}$. Consider the mapping

$$\gamma : A \times B \to A \times B/M,$$

$$(a, b) \mapsto (a\alpha^{-1}, b).$$

It is easily checked that γ is an epimorphism with $\ker \gamma = N$. Hence $A \times B/M \cong A \times B/N$. //

2.1.2 COROLLARY. *Let A, B be groups. Suppose that every automorphism of $Z(A)$ can be extended to an automorphism of A. Then the central product of A and B, amalgamating the whole of*

$Z(A)$, *is unique up to isomorphism.*

Proof. Putting $H = Z(A)$ in the above theorem, we have that $\theta\varphi^{-1} \in \text{aut } Z(A)$ and so can be extended to an automorphism of A . //

In Chapter 3, we will be concerned with irreducible linear q-groups of nilpotency class 2 where q is a fixed prime. As is well-known, an irreducible linear group has cyclic centre (2.2, Chapter 3, Gorenstein [9]), and the further restriction of class 2 makes it possible to classify such groups, as abstract groups, completely. In this direction we have

2.1.3 THEOREM (Brady, Bryce and Cossey [4]). *A finite class 2 q-group with cyclic centre is a central product either of two-generator subgroups with cyclic centre or of two-generator subgroups with cyclic centre and a cyclic subgroup.*

2.1.4 THEOREM (Brady, Bryce and Cossey [4]). *The q-groups of class 2 on two generators with cyclic centre comprise the following list:*

$$Q(\alpha, \beta)(2\beta \leq \alpha) \quad : \left\langle a, b : a^{q^\alpha} = b^{q^\beta} = 1, a^{q^{\alpha-\beta}} = [a, b] \right\rangle ;$$

$$Q(\alpha, \beta)(\beta \leq \alpha < 2\beta) : \left\langle a, b : a^{q^\alpha} = b^{q^\beta} = 1, a^{q^\beta} = [a, b]^{q^{2\beta-\alpha}}, \right.$$
$$\left. [a, b, a] = [a, b, b] = 1 \right\rangle ;$$

and if $q = 2$ we have as well

$$R(\beta)(1 \leq \beta) : \left\langle a, b : a^{2^{\beta+1}} = b^{2^{\beta+1}} = 1, a^{2^\beta} = [a, b]^{2^{\beta-1}} = b^{2^\beta}, \right.$$
$$\left. [a, b, a] = [a, b, b] = 1 \right\rangle .$$

Note that the amalgamations of the centres of the central factors in Theorem 2.1.3 must be made as large as possible. This follows from the next lemma.

2.1.5 LEMMA. *Let A, B be finite cyclic q-groups and let G be a central product of A and B such that G is cyclic. Then $G = A$ or B .*

Proof. Let A, B, C be generated by a, b, c respectively with corresponding orders q^α, q^β, q^γ . Now $G = AB$ where A centralizes

B . Hence $c = a^r b^s$, $a = c^m$, $b = c^n$ for some integers m, n, r, s , and $c = c^{mr+ns}$. Therefore $mr + ns \equiv 1 \pmod{q^\gamma}$, and so $q \nmid m$ or $q \nmid n$. It then follows that $A = \langle a \rangle = \langle c^m \rangle = \langle c \rangle = G$ or $B = G$. //

2.1.6 COROLLARY. *Let A, B be finite q-groups with cyclic centre. Let G be a central product of A and B with cyclic centre. Then the amalgamation must be made as large as possible.*

Proof. $G = AB$ where A, B centralize each other. Then $Z(G) = Z(A)Z(B)$. Clearly $Z(G)$ is a cyclic central product of two cyclic q-groups and hence by the preceding lemma, $Z(G) = Z(A)$ or $Z(B)$. //

In addition to the notations of Theorem 2.1.4, we shall find it convenient to introduce the notation $Q(\alpha, 0)$ for the cyclic group of order q^α , $\alpha > 0$. Regarding Theorem 2.1.3, a word of caution is in order here. On the face of things, there are very many central products of the groups $Q(\alpha, \beta)$ corresponding to all the different ways of amalgamating the common subgroup. However, Brady [3] has shown that if G is a finite group of class 2 with cyclic centre, then every automorphism of $Z(G)$ is the restriction to $Z(G)$ of an automorphism of G . It then follows from Corollaries 2.1.6 and 2.1.2 that all central products with cyclic centre of a given finite set of the $Q(\alpha, \beta)$ and $R(\beta)$ are, in fact, isomorphic.

In the next two sections, we will assume that q is *odd* and show that while a q-group of class 2 with cyclic centre may have many decompositions as a central product with centrally indecomposable factors, there is a canonic type of decomposition to which an analogue of the Krull-Schmidt Theorem for direct products applies.

2.2 The canonic decomposition

Henceforth $Q(n_1, r_1) \ldots Q(n_\alpha, r_\alpha)$ will always denote the central product with cyclic centre of the $Q(n_i, r_i)$, $i = 1, \ldots, \alpha$. We say that the elements a, b are *canonic generators* of $Q(n, r)$, $r > 0$, if they generate $Q(n, r)$ and satisfy the defining relations in Theorem 2.1.4. We also say the elements a_i, b_i , $i = 1, \ldots, \alpha$, are *canonic generators* of $Q(n_1, r_1) \ldots Q(n_\alpha, r_\alpha)$, where $r_i > 0$,

$i = 1, \ldots, \alpha$, if a_i, b_i are canonic generators of $Q(n_i, r_i)$, $i = 1, \ldots, \alpha$. We say that $Q(n, r)$ is of *Type* I or of *Type* II according as $2r \leq n$ or $2r > n$.

We now investigate the different ways a finite q-group of class 2 with cyclic centre decomposes.

2.2.1 LEMMA. *$Q(n_1, r_1)Q(n_2, r_2) \cong Q(n_1, r_1)Q(r_2, r_2)$ if $n_1 \geq n_2$ and $0 < r_1 \leq r_2$.*

Proof. Let $G = Q(n_1, r_1)Q(n_2, r_2)$. First we show that canonic generators may be chosen so that the following relations hold:

$$a_1^{q^{n_1-n_2+r_2}} = a_2^{q^{r_2}}, \tag{1}$$

$$[a_1, b_1] = [a_2, b_2]^{q^{r_2-r_1}}. \tag{2}$$

(i) $1 \leq r_1 \leq r_2 \leq [n_2/2] \leq [n_1/2]$.

Both $Q(n_1, r_1)$ and $Q(n_2, r_2)$ are of Type I. Thus the centre of $Q(n_i, r_i)$ is $\langle a_i^{q^{r_i}} \rangle$, $i = 1, 2$. Moreover $n_1-r_1 \geq n_2-r_2$ because $n_1-n_2 \geq 0 \geq r_1-r_2$. We then have $Z(Q(n_2, r_2)) \leq Z(Q(n_1, r_1))$. The amalgamation may be chosen to give $a_2^{q^{r_2}} = a_1^{q^{n_1-n_2+r_2}}$. Since $r_1+r_2 \leq 2[n_2/2] \leq n_2$, we have

$$[a_1, b_1] = a_1^{q^{n_1-r_1}} = \left(a_1^{q^{n_1-n_2+r_2}}\right)^{q^{n_2-r_1-r_2}} = a_2^{q^{n_2-r_1}}$$

$$= \left(a_2^{q^{n_2-r_2}}\right)^{q^{r_2-r_1}} = [a_2, b_2]^{q^{r_2-r_1}}.$$

(ii) $[n_2/2] \leq [n_1/2] < r_1 \leq r_2 \leq n_2 \leq n_1$.

Both $Q(n_1, r_1)$ and $Q(n_2, r_2)$ are of Type II, and the centre of $Q(n_i, r_i)$ is $\langle [a_i, b_i] \rangle$, $i = 1, 2$. The amalgamation may be given by $[a_1, b_1] = [a_2, b_2]^{q^{r_2-r_1}}$. Since

$r_1+r_2 > 2[n_1/2] \geq n_1 \geq n_2$, we have

$$a_2^{q^{r_2}} = [a_2, b_2]^{q^{2r_2-n_2}} = \left([a_2, b_2]^{q^{r_2-r_1}}\right)^{q^{r_1+r_2-n_2}}$$

$$= [a_1, b_1]^{q^{r_1+r_2-n_2}} = \left([a_1, b_1]^{q^{2r_1-n_1}}\right)^{q^{n_1-r_1+r_2-n_2}}$$

$$= a_1^{q^{n_1-n_2+r_2}} .$$

(iii) $1 \leq r_1 \leq [n_1/2]$, $[n_2/2] < r_2 \leq n_2$.

$Q(n_1, r_1)$ is of Type I and $Q(n_2, r_2)$ is of Type II. The centres of $Q(n_1, r_1)$, $Q(n_2, r_2)$ are $\langle a_1^{q^{r_1}} \rangle$, $[a_2, b_2]$ respectively. If $n_1-r_1 \geq r_2$, the amalgamation may be given by $a_1^{q^{n_1-r_2}} = [a_2, b_2]$, so that $a_2^{q^{r_2}} = [a_2, b_2]^{q^{2r_2-n_2}} = a_1^{q^{n_1-n_2+r_2}}$, and

$$[a_1, b_1] = a_1^{q^{n_1-r_1}} = \left(a_1^{q^{n_1-r_2}}\right)^{q^{r_2-r_1}} = [a_2, b_2]^{q^{r_2-r_1}} .$$

However, if $n_1-r_1 < r_2$, the amalgamation may be given by $a_1^{q^{r_1}} = [a_2, b_2]^{q^{r_1+r_2-n_1}}$, so that

$$a_2^{q^{r_2}} = \left([a_2, b_2]^{q^{r_1+r_2-n_1}}\right)^{q^{n_1-n_2+r_2-r_1}} = a_1^{q^{n_1-n_2+r_2}} ,$$

and

$$[a_1, b_1] = a_1^{q^{n_1-r_1}} = \left(a_1^{q^{r_1}}\right)^{q^{n_1-2r_1}} = [a_2, b_2]^{q^{r_2-r_1}} .$$

Thus we have shown that relations (1), (2) hold. Finally put $x_1 = a_1$, $y_1 = b_1 b_2^{q^{n_1-n_2+r_2-r_1}}$, $x_2 = a_1^{q^{n_1-n_2}} a_2^{-1}$, $y_2 = b_2$. Then

$$[x_2, y_1] = \left([a_1, b_1][a_2, b_2]^{-q^{r_2-r_1}}\right)^{q^{n_1-n_2}} = 1 ,$$

from relation (2). Hence $\langle x_1, y_1 \rangle$ and $\langle x_2, y_2 \rangle$ centralize each other. From relation (1), we deduce that $\langle x_2, y_2 \rangle \cong Q(r_2, r_2)$. Also $\langle x_1, y_1 \rangle \cong Q(n_1, r_1)$ and $G = \langle x_1, y_1 \rangle . \langle x_2, y_2 \rangle$. Therefore $G \cong Q(n_1, r_1)Q(r_2, r_2)$. //

2.2.2 LEMMA. *$Q(n_1, r_1)Q(n_2, r_2) \cong Q(n_1, r_1)Q(r_2, r_2)$ if $n_1-r_1 \geq n_2-r_2$, $n_1 \geq n_2$ and $r_1 > r_2 > 0$.*

Proof. With the notations in the proof of the preceding lemma, we will show that we can assume the following relations to hold:

$$a_1^{q^{n_1-n_2+r_2}} = a_2^{q^{r_2}} , \tag{1}$$

$$[a_1, b_1]^{q^{r_1-r_2}} = [a_2, b_2] . \tag{2}$$

(i) $1 \leq r_1 \leq [n_1/2]$, $1 \leq r_2 \leq [n_2/2]$.

$Q(n_1, r_1)$ and $Q(n_2, r_2)$ are of Type I. Since

$$\langle a_1^{q^{r_1}} \rangle = Z(Q(n_1, r_1)) \geq Z(Q(n_2, r_2)) = \langle a_2^{q^{r_2}} \rangle ,$$

the amalgamation may be given by $a_1^{q^{n_1-n_2+r_2}} = a_2^{q^{r_2}}$, so that

$$[a_2, b_2] = a_2^{q^{n_2-r_2}} = \left(a_2^{q^{r_2}}\right)^{q^{n_2-2r_2}} = a_1^{q^{n_1-r_2}} = \left(a_1^{q^{n_1-r_1}}\right)^{q^{r_1-r_2}}$$

$$= [a_1, b_1]^{q^{r_1-r_2}} .$$

(ii) $1 \leq r_1 \leq [n_1/2]$, $[n_2/2] < r_2 \leq n_2$.

$Q(n_1, r_1)$ is of Type I and $Q(n_2, r_2)$ is of Type II.

$$Z(Q(n_1, r_1)) = \langle a_1^{q^{r_1}} \rangle , \quad Z(Q(n_2, r_2)) = \langle [a_2, b_2] \rangle .$$

Since $r_1+r_2 < 2r_1 \leq 2[n_1/2] \leq n_1$, we have

$$Z(Q(n_1, r_1)) \geq Z(Q(n_2, r_2)) .$$

Since $r_1+r_2 < 2r_1 \le 2[n_1/2] \le n_1$, we have

$$Z(Q(n_1, r_1)) \ge Z(Q(n_2, r_2)) .$$

The amalgamation may be given by $a_1^{q^{n_1-r_2}} = [a_2, b_2]$, so that

$$a_2^{q^{r_2}} = [a_2, b_2]^{q^{2r_2-n_2}} = a_1^{q^{n_1-n_2+r_2}} , \text{ and } [a_2, b_2] = [a_1, b_1]^{q^{r_1-r_2}} .$$

(iii) $[n_1/2] < r_1 \le n_1$, $1 \le r_2 \le [n_2/2]$.

$Q(n_1, r_1)$ is of Type II and $Q(n_2, r_2)$ is of Type I. We must have $r_1 \ge n_2-r_2$; otherwise $n_1-r_1 < r_1 < n_2-r_2$, contradicting our assumptions. Thus $Z(Q(n_1, r_1)) \ge Z(Q(n_2, r_2))$, and the amalgamation may be given by $[a_1, b_1]^{q^{r_1+r_2-n_2}} = a_2^{q^{r_2}}$, so that

$$[a_2, b_2] = \left(a_2^{q^{r_2}}\right)^{q^{n_2-2r_2}} = [a_1, b_1]^{q^{r_1-r_2}} , \text{ and}$$

$$a_2^{q^{r_2}} = \left([a_1, b_1]^{q^{2r_1-n_1}}\right)^{q^{n_1-n_2+r_2-r_1}} = a_1^{q^{n_1-n_2+r_2}} .$$

(iv) $[n_1/2] < r_1 \le n_1$, $[n_2/2] < r_2 \le n_2$.

$Q(n_1, r_1)$ and $Q(n_2, r_2)$ are of Type II.

$$\langle [a_1, b_1] \rangle = Z(Q(n_1, r_1)) > Z(Q(n_2, r_2)) = \langle [a_2, b_2] \rangle .$$

The amalgamation may be given by $[a_1, b_1]^{q^{r_1-r_2}} = [a_2, b_2]$, so that

$$a_2^{q^{r_2}} = [a_2, b_2]^{q^{2r_2-n_2}} = [a_1, b_1]^{q^{r_1+r_2-n_2}}$$

$$= \left([a_1, b_1]^{q^{2r_1-n_1}}\right)^{q^{n_1-n_2+r_2-r_1}} = a_1^{q^{n_1-n_2+r_2}} .$$

To complete the proof of the lemma, put

$$x_1 = a_1 , \quad y_1 = b_1 b_2^{q^{n_1-n_2+r_2-r_1}} ,$$

$$x_2 = a_1^{q^{n_1-n_2}} a_2^{-1} , \quad y_2 = b_2 .$$

Then $[x_2, y_1] = \left([a_1, b_1]^{q^{r_1-r_2}} [a_2, b_2]^{-1}\right)^{q^{n_1-n_2+r_2-r_1}} = 1$, from relation (2). Hence $G = \langle x_1, y_1 \rangle . \langle x_2, y_2 \rangle$, where $\langle x_1, y_1 \rangle$ centralizes $\langle x_2, y_2 \rangle$, and $\langle x_1, y_1 \rangle \cong Q(n_1, r_1)$, $\langle x_2, y_2 \rangle \cong Q(r_2, r_2)$. //

2.2.3 LEMMA. *$Q(n_1, 0)Q(n_2, r_2) \cong Q(n_2, r_2)$ if $n_1 \leq r_2$ or $n_1 \leq n_2 - r_2$.*

Proof. $Q(n_1, 0) = Z(Q(n_1, 0)) \leq Z(Q(n_2, r_2))$. //

2.2.4 LEMMA. *$Q(n_1, 0)Q(n_2, r_2) \cong Q(n_1, 0)Q(r_2, r_2)$ if $n_1 \geq n_2$.*

Proof. Let $Q(n_1, 0) = \langle a_1 \rangle$, and let a_2, b_2 be canonic generators of $Q(r_2, r_2)$. The amalgamation may be given by $a_1^{q^{n_1-r_2}} = [a_2, b_2]$. Put $x_2 = a_1^{q^{n_1-n_2}} a_2$, $y_2 = b_2$. Then $\langle a_1, a_2, b_2 \rangle = \langle a_1 \rangle . \langle x_2, y_2 \rangle$, where $\langle a_1 \rangle$ centralizes $\langle x_2, y_2 \rangle \cong Q(n_2, r_2)$. //

2.2.5 LEMMA. *$Q(n_1, r_1)Q(n_2, r_2) \cong Q(n_1, r_1)Q(r_2, r_2)$ if $r_1 \geq n_2$.*

Proof. There is a q^{n_2}-cycle $C \leq Z(Q(n_1, r_1))$. Hence

$$Q(n_1, r_1)Q(n_2, r_2) = Q(n_1, r_1)CQ(n_2, r_2) \cong Q(n_1, r_1)CQ(r_2, r_2) = Q(n_1, r_1)Q(r_2, r_2)$$

using Lemma 2.2.4. //

The *canonic decomposition* for finite q-groups of class 2 with cyclic centre is now given though the proof of its uniqueness comes in the next section.

2.2.6 THEOREM. *Every non-trivial finite q-group of class 2 with cyclic centre has the central decomposition*

$$Q(l, l)^{\varepsilon_l} \ldots Q(1, 1)^{\varepsilon_1} , \quad \varepsilon_l > 0 , \quad \varepsilon_i \geq 0 , \quad i = 1, \ldots, l-1 ,$$

or $$Q(n_1, r_1) \ldots Q(n_\alpha, r_\alpha)Q(l, l)^{\varepsilon_l} \ldots Q(1, 1)^{\varepsilon_1} ,$$

$$n_1 > \ldots > n_\alpha > l , \quad n_\alpha > r_1 > \ldots > r_\alpha \geq 0 ,$$

$$0 < n_1 - r_1 < \ldots < n_\alpha - r_\alpha , \quad \varepsilon_i \geq 0 , \quad i = 1, 2, \ldots, l .$$

Proof. Let G be a non-trivial finite q-group of class 2 with cyclic centre. By Theorems 2.1.3 and 2.1.4, G has a decomposition as a product of $Q(n, r)$'s which we arrange as

$$G = Q(n_1, r_1) \ldots Q(n_\beta, r_\beta)Q(k, k)^{\lambda_k} \ldots Q(1, 1)^{\lambda_1} , \qquad (*)$$

where $n_1 \geq \ldots \geq n_\beta > 0$, $n_i > r_i > 0$ $(1 \leq i \leq \beta-1)$, $n_\beta > r_\beta \geq 0$, and where $\lambda_1, \ldots, \lambda_k \geq 0$ and $\lambda_k = 0$ implies $\lambda_1 = \ldots = \lambda_{k-1} = 0$ also.

We prove by induction on β that G has a decomposition of the type asserted. The case $\beta = 0$ is easy; so assume $\beta > 0$ and that all groups with a decomposition of the type (*) with fewer than β factors of the form $Q(n, r)$ with $n > r$ do satisfy the statement of the theorem.

First suppose that there exists $1 \leq i \leq \beta$ such that $n_i = n_{i+1}$. Then, from Lemmas 2.2.1 or 2.2.4, we have

$$Q(n_i, r_i)Q(n_{i+1}, r_{i+1}) \cong Q(n_i, r)Q(s, s)$$

where $r = \min\{r_i, r_{i+1}\}$, $s = \max\{r_i, r_{i+1}\}$. Hence G has a decomposition with $\beta - 1$ factors of the form $Q(n, r)$ with $n > r$ and so by induction, we are done. We may therefore suppose that

$$n_1 > n_2 > \ldots > n_\beta > 0 .$$

If, for some $1 \leq i \leq \beta$, either $r_i \leq r_{i+1}$, or $r_i > r_{i+1}$, but $n_i - r_i \geq n_{i+1} - r_{i+1}$, then using Lemmas 2.2.1, 2.2.2 or 2.2.3, we again give G a decomposition with fewer than β $Q(n, r)$'s with $n > r$. Hence we may assume that

$$r_1 > r_2 > \ldots > r_\beta \geq 0$$

and

$$0 < n_1 - r_1 < \ldots < n_\beta - r_\beta \ .$$

Finally if $\lambda_k \neq 0$ and $n_\beta \leq k$, then using Lemma 2.2.5, $Q(n_\beta, r_\beta)Q(k, k) \cong Q(k, k)Q(r_\beta, r_\beta)$, and we may again use induction. Hence we may assume $n_\beta > k$; and if $n_\alpha \leq r_1$, use Lemma 2.2.5 again. The induction is now complete. //

An easy observation of the reduction process in the proof of the above theorem gives the following corollary which will be of use in 4.2.

2.2.7 COROLLARY. *Suppose G is a central product with cyclic centre of λ central factors of the type $Q(r, r)$ and a finite set of $Q(n, r)$'s. Then the canonic decomposition of G contains at least λ central factors of the type $Q(r, r)$.*

2.3 Uniqueness of the canonic decomposition

In this section G and H will always denote non-trivial finite q-groups of class 2 with cyclic centre. We write $G = G_* G_0$ where $G_* = Q(n_1, r_1) \ldots Q(n_\alpha, r_\alpha)$ and $G_0 = Q(1, 1)^{\varepsilon_1} \ldots Q(1, 1)^{\varepsilon_1}$, satisfying the conditions of the canonic decomposition in Theorem 2.2.6 and allowing $\alpha = 0$, in which case $G_* = 1$. Similarly for the notation $H = H_* H_0$. For any finite q-group A, we use the notations:

$$\Omega^i(A) = \langle x^{q^i} : x \in A \rangle \ , \quad i \geq 0 \ ,$$

$$d(A) = \text{minimal number of generators of } A \ .$$

For $i \geq 0$, we define the numbers $\rho_i(G)$ and $\sigma_i(G)$ as follows:

$$\rho_i(G) = \begin{cases} d\left(\Omega^i(G/Z(G))\right) & \text{if } \Omega^i(G/Z(G)) \neq 1 \ , \\ 0 & \text{if } \Omega^i(G/Z(G)) = 1 \ ; \end{cases}$$

$$\sigma_i(G) = \begin{cases} d\left(\Omega^i(G)/\Omega^i(G')\right) & \text{if } \Omega^i(G)/\Omega^i(G') \neq 1 \ , \\ 0 & \text{if } \Omega^i(G)/\Omega^i(G') = 1 \ . \end{cases}$$

These numbers are clearly isomorphism invariants and will play an important role in the proof of the uniqueness of the canonic decomposition. We can easily calculate $\rho_i(G)$ from the following lemmas.

2.3.1 LEMMA. *Let GH be the central product of G and H with cyclic centre. Then $\rho_i(GH) = \rho_i(G) + \rho_i H$, $i \geq 0$.*

Proof. Since the centre of GH is cyclic, we may assume that $Z(G) \geq Z(H)$. If $GH = G$, then $H \leq Z(G)$ and so H is cyclic. By definition, $\rho_i(H) = 0$ and hence $\rho_i(GH) = \rho_i(G) + \rho_i(H)$. Similarly for the case when $GH = H$.

So suppose that $GH \neq G$ and $GH \neq H$. Then

$$\Omega^i\{GH/Z(GH)\} = \Omega^i\{G/Z(G)\}.\Omega^i\{HZ(G)/Z(G)\} .$$

We claim that $\Omega^i\{G/Z(G)\} \cap \Omega^i\{HZ(G)/Z(G)\} = 1$. For if $\overline{x}$ belongs to this intersection, then $\overline{x} = g^{q^i} Z(G) = h^{q^i} Z(G)$ for some $g \in G$, $h \in H$, and hence $h^{q^i} \in G \cap H = Z(H) \leq Z(G)$, and so $\overline{x} = 1$. Also $HZ(G)/Z(G) \cong H/H \cap Z(G) = H/Z(H)$. Since all the factor groups dealt with are abelian q-groups, we have the required result. //

2.3.2 LEMMA. *For $i \geq 0$, $j \geq 0$,*

$$\rho_i\{Q(n_1, r_1) \ldots Q(n_j, r_j)\} = \rho_i\{Q(n_1, r_1)\} + \ldots + \rho_i\{Q(n_j, r_j)\} .$$

Proof. Follows from Lemma 2.3.1 by an easy induction.

2.3.3 LEMMA.

$$\rho_i\{Q(n, r)\} = \begin{cases} 2 & \text{if } 0 \leq i < r , \\ 0 & \text{if } i \geq r . \end{cases}$$

Proof. If $r = 0$, there is nothing to prove. So suppose $r > 0$. Let $G = Q(n, r) = \langle a, b \rangle$. Then, for $0 \leq i < r$, $a^{q^i}, b^{q^i} \notin Z(G)$, and $\langle a^{q^i} Z(G) \rangle \cap \langle b^{q^i} Z(G) \rangle = 1$, so that $\Omega^i\{G/Z(G)\} = \langle a^{q^i} Z(G) \rangle \times \langle b^{q^i} Z(G) \rangle$. However, for $i \geq r$, $a^{q^i} \in Z(G)$ and $b^{q^i} = 1$, and hence

$$\Omega^i(G/Z(G)) = 1 . \qquad //$$

The computation of $\sigma_i(G)$ is more complicated, and it is useful to introduce the auxiliary constants $\sigma_i(G_*)$, $\sigma_i(G_0)$, $i \geq 0$, corresponding to each G , defined by:

$$\sigma_i(G_*) = \begin{cases} d(\Omega^i(G_*)\Omega^i(G')/\Omega^i(G')) & \text{if } \Omega^i(G_*)\Omega^i(G')/\Omega^i(G') \neq 1 , \\ 0 & \text{if } \Omega^i(G_*)\Omega^i(G')/\Omega^i(G') = 1 ; \end{cases}$$

$$\sigma_i(G_0) = \begin{cases} d(\Omega^i(G_0)/\Omega^i(G_0')) & \text{if } \Omega^i(G_0)/\Omega^i(G_0') \neq 1 , \\ 0 & \text{if } \Omega^i(G_0)/\Omega^i(G_0') = 1 . \end{cases}$$

Their relevance is given by the next lemma.

2.3.4 LEMMA. $\sigma_i(G) = \sigma_i(G_*) + \sigma_i(G_0)$, $i \geq 0$.

Proof. Trivial if $G_0 = 1$. So suppose that $G_0 \neq 1$. Write $N = \Omega^i(G')$, $A = \Omega^i(G_*)N/N$, $B = \Omega^i(G_0)N/N$, so that $\Omega^i(G)/\Omega^i(G') = AB$.

We claim that $A \cap B = 1$. Let $\overline{x} = xN \in A \cap B$ and we may suppose $x \in \Omega^i(G_0)$. Then x is central in G , and hence $x \in \Omega^i(G_0) \cap Z(G_0) = \Omega^i(G_0) \cap G_0'$. If we could show that

$$\Omega^i(G_0) \cap G_0' = \Omega^i(G_0') , \qquad (*)$$

then $\overline{x} = 1$. To do this, let

$$Q(j, j)^{\varepsilon_j} = \langle a_{jk}, b_{jk} : k = 1, \ldots, \varepsilon_j \rangle , \quad j = 1, \ldots, l ; \quad \varepsilon_l > 0 .$$

Let $y \in \Omega^i(G_0)$. Then

$$y = \left(\prod_{j=i+1}^{l} \prod_{k=1}^{\varepsilon_j} a_{jk}^{\lambda_{jk}q^i} b_{jk}^{\mu_{jk}q^i} \right) [a_{l1}, b_{l1}]^{\nu q^i} .$$

If $y \in G_0'$, then y is central in G_0 . Commuting with a_{jk} and

b_{jk} , we get $1 = [a_{jk}, b_{jk}]^{\lambda_{jk}q^i} = [a_{jk}, b_{jk}]^{\mu_{jk}q^i}$. Hence q^i divides $\lambda_{jk}q^i$ and $\mu_{jk}q^i$, and so $y = [a_{l1}, b_{l1}]^{\nu q^i} \in \Omega^i(G_0')$. Therefore (*) is proved.

Finally, $B \cong \Omega^i(G_0)/\Omega^i(G_0) \cap N$, and it may be shown as in above that $\Omega^i(G_0) \cap N = \Omega^i(G_0)$. Since AB is an abelian q-group, we have the lemma. //

We require a few preliminary results.

2.3.5 LEMMA. *Canonic generators* a_i, b_i , $i = 1, 2$, *of* $Q(n_1, r_1)Q(n_2, r_2)$ *where* $n_1 > n_2 > r_1 > r_2 > 0$, $n_1-r_1 < n_2-r_2$, *may be chosen so that the following relations hold:*

$$a_1^{q^{r_1}} = a_2^{q^{n_2-n_1+r_1}},$$

$$[a_1, b_1]^{q^{r_1-r_2}} = [a_2, b_2] .$$

Proof. The details of the proof are those in the proof of Lemma 2.2.1. We have to consider 3 cases:

(i) $Q(n_1, r_1)$ and $Q(n_2, r_2)$ are both of Type I,

(ii) $Q(n_1, r_1)$ and $Q(n_2, r_2)$ are both of Type II,

(iii) $Q(n_1, r_1)$ is of Type II and $Q(n_2, r_2)$ is of Type I.

Note that it is not possible to have $Q(n_1, r_1)$ of Type I and $Q(n_2, r_2)$ of Type II because it would then mean that $r_1 \leq n_1-r_1 < n_2-r_2 < r_2$, contradicting the assumption that $r_1 > r_2$. //

2.3.6 LEMMA. *Let* $Q(n_2, 0) = \langle a_2 \rangle$. *Then canonic generators* a_1, b_1 *of* $Q(n_1, r_1)$ *may be chosen so that the following relation holds in* $Q(n_1, r_1)Q(n_2, 0)$ *where* $n_1 > n_2 > r_1 > 0$, $n_1-r_1 < n_2$:

$$a_1^{q^{r_1}} = a_2^{q^{n_2-n_1+r_1}} .$$

Proof. Routine. //

In the rest of this section, we denote the canonic generators of $G_* = Q(n_1, r_1) \ldots Q(n_\alpha, r_\alpha)$ by a_i, b_i, $i = 1, \ldots, \alpha$. If $r_\alpha = 0$, we set $b_\alpha = 1$.

2.3.7 LEMMA. *Let* $r \geq n_{i+1}-n_i+r_i$, $1 \leq i < \alpha$. *Then*

$$\Omega^r(G_*) = \Omega^r(Q(n_1, r_1) \ldots Q(n_i, r_i)) .$$

Proof. Let $1 \leq i < j \leq \alpha$. We have, by Lemmas 2.3.5 and 2.3.6,

$$a_i^{q^{r_i}} = a_j^{q^{n_j-n_i+r_i}} .$$

Since $r \geq n_{i+1}-n_i+r_i \geq n_j-n_i+r_i$, we have

$$a_j^{q^r} = a_i^{q^{r+n_i-n_j}} \in \Omega^r(Q(n_i, r_i)) .$$

Also $r \geq n_{i+1}-n_i+r_i > r_{i+1} \geq r_j$ and hence $b_j^{q^r} = 1$.

Hence $\Omega^r(Q(n_j, r_j)) \leq \Omega^r(Q(n_i, r_i))$ for $i < j \leq \alpha$.

2.3.8 COROLLARY. *Let* $r \geq r_{i+1}$, $0 \leq i < \alpha$. *Then*

$$\Omega^r(G_*) = \Omega^r(Q(n_1, r_1) \ldots Q(n_{i+1}, r_{i+1})) .$$

Proof. If $i = \alpha - 1$, there is nothing to prove. If $i < \alpha - 1$, then $r_{i+1} > n_{i+2}-n_{i+1}+r_{i+1}$ and the corollary follows from Lemma 2.3.7. //

2.3.9 LEMMA. *Let* $r \geq 0$. *If* $a_i^{q^r} \neq 1$, *then* $a_i^{q^r} \notin \Omega^r(G')$.

Proof. $G' = G'_*$ or G'_0 according as $r_1 \geq l$ or $r_1 < l$.

Hence $|\Omega^r(G')| = 1$ or q^{m-r}, where $m = \max\{r_1, l\}$, according as $r \geq m$ or $r < m$.

If $r \geq m$, clearly $a_i^{q^r} \notin \Omega^r(G')$. If $r < m$, suppose that $a_i^{q^r} \in \Omega^r(G')$; then $a_i^{q^m} = \left(a_i^{q^r}\right)^{q^{m-r}} = 1$, which is a contradiction since $m < n_i$ for $i = 1, \ldots, \alpha$. Hence $a_i^{q^r} \notin \Omega^r(G')$. //

We can now calculate $\sigma_i(G_*)$, $\sigma_i(G_0)$, $i \geq 0$.

2.3.10 LEMMA.

$$\sigma_r(G_0) = \begin{cases} 2(\varepsilon_l + \ldots + \varepsilon_{r+1}) & \text{if } l > r \geq 0, \\ 0 & \text{if } r \geq l. \end{cases}$$

Proof. Recall that $G_0 = Q(l, l)^{\varepsilon_l} \ldots Q(1, 1)^{\varepsilon_1}$, $\varepsilon_i \geq 0$, $i = 1, \ldots, l$. We may assume that $\varepsilon_l > 0$. If $r \geq l$, then $\Omega^r(G_0) = 1 = \Omega^r(G_0')$ and hence $\sigma_r(G_0) = 0$.

So suppose $0 \leq r < l$. Write

$$Q_i = Q(i, i)^{\varepsilon_i} = \langle x_{ij}, y_{ij} : j = 1, \ldots, \varepsilon_i \rangle, \quad i = 1, \ldots, l.$$

Then $\Omega^r(G_0) = \Omega^r(Q_l \ldots Q_{r+1})$, $\Omega^r(G_0') = \Omega^r(Q_l')$. Write

$$P_i = \Omega^r(Q_i)\Omega^r(Q_l')/\Omega^r(Q_l'), \quad i = 1, \ldots, l.$$

Clearly $P_i = 1$ for $i \leq r$. We now show that

$$P_i \cong \Omega^r(Q_i)/\Omega^r(Q_i'), \quad i = 1, \ldots, l.$$

We may suppose that $i > r$. It is sufficient to prove that

$$\Omega^r(Q_i) \cap \Omega^r(Q_l') = \Omega^r(Q_i').$$

Let $x \in \Omega^r(Q_i) \cap \Omega^r(Q_l')$ where

$$x = \left(\prod_{j=1}^{\varepsilon_i} x_{ij}^{\lambda_j q^r} y_{ij}^{\mu_j q^r}\right) [x_{i1}, y_{i1}]^{\nu q^r}.$$

Then x is central in Q_i. Commuting with x_{ij} and y_{ij}, we have

$$1 = [x_{ij}, y_{ij}]^{\lambda_j q^r} = [x_{ij}, y_{ij}]^{\mu_j q^r} .$$

Hence q^i divides $\lambda_j q^r$ and $\mu_j q^r$ and so $x = [x_{i1}, y_{i1}]^{\nu q^r} \in \Omega^r(Q_i')$.

Finally we claim that for $l \geq i > r$,

$$P_i \cap P_l \ldots P_{i+1} P_{i-1} \ldots P_{r+1} = 1 .$$

For let $\overline{y}$ belong to this intersection, where we may assume $y \in \Omega^r(Q_i)$, so that

$$y = \left(\prod_{j=1}^{\varepsilon_i} x_{ij}^{\xi_j q^r} y_{ij}^{\eta_j q^r} \right) [x_{i1}, y_{i1}]^{\zeta q^r} ,$$

and

$$y = y_l \ldots y_{i+1} y_{i-1} \ldots y_{r+1} y' ,$$

where $y_i \in \Omega^r(Q_i)$, $y' \in \Omega^r(Q_l')$. Hence y is central in Q_i . Again, commuting y with x_{ij} and y_{ij} , we have

$$1 = [x_{ij}, y_{ij}]^{\xi_j q^r} = [x_{ij}, y_{ij}]^{\eta_j q^r} ,$$

and hence q^i divides $\xi_j q^r$ and $\eta_j q^r$. Therefore $y = [x_{i1}, y_{i1}]^{\zeta q^r} \in \Omega^r(Q_i')$ and so $\overline{y} = 1$.

It is clear that for $l \geq i > r$,

$$\Omega^r(Q_i)/\Omega^r(Q_i') = \left\langle \overline{x_{i1}}^{q^r} \right\rangle \times \left\langle \overline{y_{i1}}^{q^r} \right\rangle \times \ldots \times \left\langle \overline{x_{i\varepsilon_i}}^{q^r} \right\rangle \times \left\langle \overline{y_{i\varepsilon_i}}^{q^r} \right\rangle ,$$

and hence $d(P_i) = 2\varepsilon_i$, $i = r+1, \ldots, l$. Since

$$\Omega^r(G_0)/\Omega^r(G_0') = P_l \times P_{l-1} \times \ldots \times P_{r+1} ,$$

we have $\sigma_r(G_0) = 2(\varepsilon_l + \ldots + \varepsilon_{r+1})$. //

2.3.11 LEMMA. *Let* $n_{i+1} - n_i + r_i \leq r < r_i$, $1 \leq i < \alpha$. *Then* $\sigma_r(G_*) = 2i$.

Proof. By Lemma 2.3.7, $\Omega^r(G_*) = \Omega^r\left(Q(n_1, r_1) \ldots Q(n_i, r_i)\right)$. Write

$$P = \Omega^r(G_*)\Omega^r(G')/\Omega^r(G')$$
$$= \left\langle \overline{a_1}^{q^r}, \overline{b_1}^{q^r}, \ldots, \overline{a_i}^{q^r}, \overline{b_i}^{q^r} \right\rangle .$$

We claim that the set $S = \left\{\overline{a_j}^{q^r}, \overline{b_j}^{q^r}, j = 1, \ldots, i\right\}$ is a minimal set of generators for P. If not, we can eliminate at least one element x from S. Suppose $x = \overline{b_j}^{q^r}$ for some $1 \le j \le i$. Then x can be expressed in terms of the other generators, and since $\Omega^r(G') \le Z(G)$, we have $1 = \left[a_j, b_j^{q^r}\right] = [a_j, b_j]^{q^r}$, contradicting the assumption that $r < r_i \le r_j$. On the other hand, if $x = \overline{a_j}^{q^r}$ for some $1 \le j \le i$, we can similarly show that $[a_j, b_j]^{q^r} = 1$, which is again impossible. Hence S is a minimal set. Since P is an abelian q-group, we have $d(P) = 2i$. //

2.3.12 LEMMA. *Suppose that* $r_\alpha > 0$. *Let* $0 \le r < r_\alpha$. *Then* $\sigma_r(G_*) = 2\alpha$.

Proof. Similar to the proof of the preceding lemma. //

2.3.13. LEMMA. *Let* $r_{i+1} \le r < n_{i+1} - n_i + r_i$, $0 \le i < \alpha$, *where we set* $n_0 = r_0 = 0$. *Then* $\sigma_r(G_*) = 2i + 1$.

Proof. By Corollary 2.3.8, $\Omega^r(G_*) = \Omega^r\left(Q(n_1, r_1) \ldots Q(n_{i+1}, r_{i+1})\right)$. Write

$$P = \Omega^r(G_*)\Omega^r(G')/\Omega^r(G')$$
$$= \left\langle \overline{a_1}^{q^r}, \ldots, \overline{a_{i+1}}^{q^r}, \overline{b_1}^{q^r}, \ldots, \overline{b_i}^{q^r} \right\rangle .$$

We claim that the set $S = \left\{\overline{a_1}^{q^r}, \ldots, \overline{a_{i+1}}^{q^r}, \overline{b_1}^{q^r}, \ldots, \overline{b_i}^{q^r}\right\}$ is a minimal set of generators for P. If not, we can delete at least one

element x from S. Suppose that $x = a_j^{q^r}$ or $b_j^{q^r}$ for some $1 \le j \le i$. Then x can be expressed in terms of the other generators, and since $\Omega^r(G') \le Z(G)$, we have that $[a_j, b_j]^{q^r} = 1$ in either case. This contradicts the assumption that $r < n_{i+1} - n_i + r_i < r_i \le r_j$. So suppose $x = a_{i+1}^{q^r}$. We then proceed as follows. We would have $a_{i+1}^{q^r} = a_1^{\lambda_1 q^r} \dots a_i^{\lambda_i q^r} b_1^{\mu_1 q^r} \dots b_i^{\mu_i q^r} c$ for some $c \in \Omega^r(G')$. Commuting both sides with a_j and b_j, $1 \le j \le i$, we get

$$1 = [a_j, b_j]^{\lambda_j q^r} = [a_j, b_j]^{\mu_j q^r}.$$

Hence q^{r_j} divides $\lambda_j q^r$ and $\mu_j q^r$, and so $q^{r_j - r} \mid \lambda_j, \mu_j$. Write $\lambda_j = \lambda'_j q^{r_j - r}$, $\mu_j = \mu'_j q^{r_j - r}$, $j = 1, \dots, i$. Then

$$\begin{aligned} a_{i+1}^{q^r} &= a_1^{\lambda'_1 q^{r_1}} \dots a_i^{\lambda'_i q^{r_i}} b_1^{\mu'_1 q^{r_1}} \dots b_i^{\mu'_i q^{r_i}} c \\ &= a_1^{\lambda'_1 q^{r_1}} \dots a_i^{\lambda'_i q^{r_i}} c. \end{aligned}$$

By Lemmas 2.3.5 and 2.3.6, we may suppose that

$$a_j^{q^{r_j}} = a_{i+1}^{q^{n_{i+1} - n_j + r_j}}, \quad j = 1, \dots, i.$$

Hence

$$a_{i+1}^{q^r} = a_{i+1}^{\lambda'_1 q^{n_{i+1} - n_1 + r_1}} \dots a_{i+1}^{\lambda'_i q^{n_{i+1} - n_i + r_i}} c,$$

or $\left(a_{i+1}^{\lambda}\right)^{q^r} \in \Omega^r(G')$, where

$$\lambda = 1 - \lambda'_1 q^{n_{i+1} - n_1 + r_1 - r} - \dots - \lambda'_i q^{n_{i+1} - n_i + r_i - r}.$$

Since $r < n_{i+1}-n_i+r_i < \ldots < n_{i+1}-n_1+r_1$, it follows that λ is prime to q , and hence $a_{i+1}^{q^r} \in \Omega^r(G')$, which contradicts Lemma 2.3.9 since $a_{i+1}^{q^r} \neq 1$. Thus we have proved the minimality of S and so $d(P) = 2i + 1$. //

We will be concerned only with the parity of $\sigma_r(G)$. This is given by

2.3.14 THEOREM. *$\sigma_r(G)$ is even if $n_{i+1}-n_i+r_i \leq r < r_i$, $1 \leq i < \alpha$, or if $0 \leq r < r_\alpha$ (when $r_\alpha > 0$).*

$\sigma_r(G)$ is odd if $r_{i+1} \leq r < n_{i+1}-n_i+r_i$, $0 \leq i < \alpha$, where we set $n_0 = r_0 = 0$.

Proof. Since for all $r \geq 0$, $\sigma_r(G) = \sigma_r(G_*) + \sigma_r(G_0)$ and $\sigma_r(G_0)$ is even, by Lemmas 2.3.4 and 2.3.10, it follows that $\sigma_r(G)$ and $\sigma_r(G_*)$ are of the same parity. The theorem then follows from Lemmas 2.3.11, 2.3.12 and 2.3.13. //

Since $\sigma_r(G)$, $r \geq 0$, are isomorphism invariants, the next lemma is clear.

2.3.15 LEMMA. *If $G \cong H$, then $\sigma_r(G)$ and $\sigma_r(H)$ are of the same parity for $r \geq 0$.*

We can now prove the main result of this chapter.

2.3.16 THEOREM. *The canonic decomposition for finite q-groups of class 2 with cyclic centre as given in Theorem 2.2.6 is unique up to isomorphism.*

Proof. Let G and H be non-trivial finite q-groups of class 2 with cyclic centre expressed in canonic decompositions

$$G = Q(n_1, r_1) \ldots Q(n_\alpha, r_\alpha)Q(l, l)^{\varepsilon_l} \ldots Q(1, 1)^{\varepsilon_1} = G_*G_0 ,$$

$$H = Q(m_1, s_1) \ldots Q(m_\beta, s_\beta)Q(k, k)^{\varepsilon_k} \ldots Q(1, 1)^{\varepsilon_1} = H_*H_0 .$$

It is trivial that $G \cong H$ if $\alpha = \beta$, $l = k$, $n_i = m_i$ and $r_i = s_i$

for $i = 1, \ldots, \alpha$, and $\varepsilon_i = \delta_i$ for $i = 1, \ldots, l$.

So assume that $G \tilde{=} H$.

Step 1. $\alpha = 0$. In this case, $G_* = 1$. Suppose that $\beta > 0$. Then, by Lemma 2.3.10, $\sigma_{s_1}(G)$ is even while, by Lemma 2.3.14, $\sigma_{s_1}(H)$ is odd, contradicting Lemma 2.3.15. Hence $\beta = 0$.

We may then assume that $\varepsilon_l > 0$, $\delta_k > 0$. Suppose $l > k$; then by Lemmas 2.3.2 and 2.3.3,

$$\rho_k(G) = 2(\varepsilon_l + \ldots + \varepsilon_{l+1}) > 0 = \rho_k(H),$$

where is a contradiction since $\rho_k(G)$ is an isomorphism invariant. Hence $l = k$. From the relations $\rho_i(G) = \rho_i(H)$, $i = 0, 1, \ldots, l-1$, we have

$$\varepsilon_l + \ldots + \varepsilon_1 = \delta_l + \ldots + \delta_1,$$

$$\varepsilon_l + \ldots + \varepsilon_2 = \delta_l + \ldots + \delta_2,$$

$$\ldots\ldots\ldots$$

$$\varepsilon_l = \delta_l.$$

Hence $\varepsilon_i = \delta_i$, $i = 1, \ldots, l$.

In the rest of this proof, we assume $\alpha > 0$.

Step 2. We prove: $n_1 = m_1$, $r_1 = s_1$.

By Step 1, β cannot be zero and so $\beta > 0$. Clearly $q^{n_1} = q^{m_1}$ = exponent of G and hence $n_1 = m_1$. If $r_1 \neq s_1$, we may suppose that $r_1 > s_1$. Then either $r_\alpha > s_1$ or $r_\gamma > s_1 \geq r_{\gamma+1}$ for some $1 \leq \gamma < \alpha$. If $r_\alpha > s_1$, then by Theorem 2.3.14, $\sigma_{s_1}(G)$ is even and $\sigma_{s_1}(H)$ is odd, contradicting Lemma 2.3.15. However, if $r_\gamma > s_1 \geq r_{\gamma+1}$ for some $1 \leq \gamma < \alpha$, let $s = \max\{n_{\gamma+1} - n_\gamma + r_\gamma, s_1\}$ so that $s_1 \leq s < m_1$ and $n_{\gamma+1} - n_\gamma + r_\gamma \leq s < r_\gamma$. Hence by Theorem 2.3.14, $\sigma_s(H)$ is odd and $\sigma_s(G)$ is even, again contradicting Lemma

2.3.15. Hence $r_1 = s_1$.

Since we will be referring frequently to Theorem 2.3.14 and Lemma 2.3.15 and it is clear from the context that one or the other is being invoked, we will, for brevity, omit references to them.

Step 3. We prove: if $n_i = m_i$, $r_i = s_i$, $i = 1, \ldots, \nu$, where $\nu < \min\{\alpha, \beta\}$, then $n_{\nu+1} = m_{\nu+1}$, $r_{\nu+1} = s_{\nu+1}$.

First we show that $r_{\nu+1} = s_{\nu+1}$. If not, assume that $r_{\nu+1} > s_{\nu+1}$.

Claim A: $n_{\nu+1} = m_{\nu+1}$.

Let $u = n_{\nu+1} - n_\nu + r_\nu$, $v = m_{\nu+1} - m_\nu + s_\nu$. Now $s_\nu > r_{\nu+1} > s_{\nu+1}$ and $s_\nu > v > s_{\nu+1}$. Either $s_\nu > r_{\nu+1} \geq v$ or $v > r_{\nu+1} > s_{\nu+1}$. In the first case, $\sigma_{r_{\nu+1}}(H)$ is even and $\sigma_{r_{\nu+1}}(G)$ is odd: a contradiction. We must then have $s_\nu > v > r_{\nu+1} > s_{\nu+1}$, or $r_\nu > v > r_{\nu+1}$ since $r_\nu = s_\nu$. Also $r_\nu > u > r_{\nu+1}$. If $r_\nu > v > u > r_{\nu+1}$, then $\sigma_u(G)$ is even and $\sigma_u(H)$ is odd: a contradiction. However, if $r_\nu > u > v > r_{\nu+1}$ then $\sigma_v(G)$ is odd and $\sigma_v(H)$ is even: a contradiction. Hence $u = v$, and so $n_{\nu+1} = m_{\nu+1}$.

Claim B: $r_\lambda > s_{\nu+1} \geq r_{\lambda+1}$ for some $\nu < \lambda < \alpha$.

This is clear if $r_\alpha = 0$. So suppose $r_\alpha > 0$. If the claim is false, then $r_\alpha > s_{\nu+1}$, so that $\sigma_{s_{\nu+1}}(G)$ is even and $\sigma_{s_{\nu+1}}(H)$ is odd: a contradiction.

Finally we show that Claim B leads to a contradiction. Let $w = n_{\lambda+1} - n_\lambda + r_\lambda$. Then $w < u = v$ for we have $u - w = (n_{\nu+1} - n_{\lambda+1}) + (n_\lambda - n_\nu + r_\nu - r_\lambda) > 0$ since $\nu < \lambda$. Now $r_\lambda > w > r_{\lambda+1}$ and $r_\lambda > s_{\nu+1} \geq r_{\lambda+1}$. Either $r_\lambda > s_{\nu+1} \geq w$ or $w > s_{\nu+1} \geq r_{\lambda+1}$. The first case implies that $\sigma_{s_{\nu+1}}(G)$ is even and

$\sigma_{s_{\nu+1}}(H)$ is odd. The other case implies that $\sigma_w(H)$ is odd and $\sigma_w(G)$ is even. Both cases lead to contradictions. Hence we must have $r_{\nu+1} = s_{\nu+1}$.

To complete Step 3, we now prove that $n_{\nu+1} = m_{\nu+1}$. If not, assume that $n_{\nu+1} > m_{\nu+1}$. Then, with u and v defined as in the proof of Claim A, we have $u > v > s_{\nu+1} = r_{\nu+1}$. Thus $\sigma_v(G)$ is odd $\sigma_v(H)$ is even: a contradiction. Hence $n_{\nu+1} = m_{\nu+1}$.

Step 4. We prove: $\alpha = \beta$.

If not, assume that $\alpha > \beta$, By Step 3, we have $n_i = m_i$, $r_i = s_i$ for $i = 1, \ldots, \beta$. Thus $r_{\beta+1} < s_\beta$, and hence $\sigma_{r_{\beta+1}}(G)$ is odd, and $\sigma_{r_{\beta+1}}(H)$ is even: a contradiction. Of course, if $s_\beta = 0$, then $r_\beta = 0$ and so α must be equal to β.

At this point of the proof, we have $\alpha = \beta$, $n_i = m_i$, $r_i = s_i$, $i = 1, \ldots, \alpha$, or $G_* \cong H_*$.

Step 5. We prove: $l = k$, $\varepsilon_i = \delta_i$, $i = 1, \ldots, l$.

First we show that $G_0 = 1$ implies $H_0 = 1$. For if $H_0 \neq 1$, we may suppose $\delta_k > 0$, and since $G_* \cong H_*$, we have by Lemma 2.3.1, $\rho_0(G_0) = \rho_0(H_0)$, and so by Lemmas 2.3.2 and 2.3.3, $2(\delta_k + \ldots + \delta_1) = 0$, which contradicts our assumption. Hence $H_0 = 1$.

Lastly we assume $\varepsilon_l > 0$, $\delta_k > 0$. As in Step 1, it is easily shown that $l = k$, $\varepsilon_i = \delta_i$, $i = 1, \ldots, l$. The proof is then complete. //

The uniqueness of the canonic decomposition for finite q-groups of class 2 with cyclic centre enables us to classify the closed classes of irreducible linear groups in $\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_{q^i}$. This classification will be given in the next chapter.

CHAPTER 3

THE IRREDUCIBLE LINEAR GROUPS IN $\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_{q^n}$

3.1 Preliminaries

We will consider an irreducible linear group over a field E as an abstract group A together with a faithful irreducible EA-module U which is unique up to linear isomorphism. In this section the abstract group A under consideration belongs to $\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_{q^n}$ for some fixed integer $n > 0$ and E is a field whose characteristic is prime to q. Under these conditions, a theorem of Brady, Bryce and Cossey [4] tells us that all faithful irreducible EA-modules are linearly isomorphic, and the choice of the faithful irreducible EA-module U is immaterial. We then denote the irreducible linear group corresponding to A and U by A^E, to emphasize the field E and distinguish the linear group from the abstract group A. Clearly A^E is uniquely determined by the abstract group A and the field E.

We define a linear factor of A^E as in 1.2. B^E is a *linear factor* of A^E (written $B^E \prec A^E$) if there exists $A_0 \leq A$ such that $A_0/\ker U_j \cong B$ as abstract groups for some irreducible EA_0-module U_j, $1 \leq j \leq r$, in the decomposition, $U_{A_0} = U_1 \oplus \ldots \oplus U_r$, into irreducible EA_0-modules U_i, where U is the faithful irreducible EA-module.

In this section we denote $GF(p)$ by K, where p is prime to q. We will show that we only need to consider the irreducible linear groups in $\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_{q^n}$ over a suitable splitting field.

3.1.1 LEMMA. *Let A be any finite q-group with cyclic centre and $A \in \underline{\underline{N}}_2 \wedge \underline{\underline{B}}_{q^n}$. Then there is a finite normal extension L of K such that L is a splitting field for A.*

Proof. Let q^m be the exponent of A so that $0 \leq m \leq n$. Let ω_i, $i > 0$, denote a primitive q^i-th root of unity. Then $K(\omega_m)$

is a splitting field for A (70.24, Curtis and Reiner [6]). Since $K(\omega_n)$ is a finite extension of K, we have by 49.5.1, Warner [25], that there is an extension L of $K(\omega_n)$ which is a finite normal extension of K. Moreover $L \supseteq K(\omega_n) \supseteq K(\omega_m)$ and hence L is a splitting field for A. //

In the rest of this section L will always denote the finite normal extension of K in the above lemma, and will be kept fixed.

3.1.2 LEMMA. *$B^K \prec A^K$ if and only if $B^L \prec A^L$.*

Proof. Let U be a faithful irreducible KA-module. If $B^K \prec A^K$, then there exists $A_0 \leq A$ such that $U_{A_0} = U_1 \oplus \ldots \oplus U_r$, where the U_i are irreducible KA_0-modules, and $A_0/\ker U_1 \cong B$ as abstract groups. By 70.15, Curtis and Reiner [6], we have

$$U^L = V_1 \oplus \ldots \oplus V_s ,$$

where the V_i are irreducible LA-modules and are Galois conjugates of each other, and so $\ker V_1 = \ldots = \ker V_s = 1$. Hence the V_i are linearly isomorphic faithful irreducible LA-modules. Now

$$\begin{aligned} (U^L)_{A_0} &= (V_1)_{A_0} \oplus \ldots \oplus (V_s)_{A_0} \\ &= \left(V_{11} \oplus \ldots \oplus V_{1t_1}\right) \oplus \ldots \oplus \left(V_{s1} \oplus \ldots \oplus V_{st_s}\right) , \end{aligned}$$

where the V_{ij} are irreducible LA_0-modules. Also

$$\begin{aligned} \left(U_{A_0}\right)^L &= U_1^L \oplus \ldots \oplus U_r^L \\ &= \left(U_{11} \oplus \ldots \oplus U_{1m_1}\right) \oplus \ldots \oplus \left(U_{r1} \oplus \ldots \oplus U_{rm_r}\right) , \end{aligned}$$

where the U_{ij} are irreducible LA_0-modules and $\ker U_{ij} = \ker U_i$. Applying the Krull-Schmidt Theorem to $(U^L)_{A_0} = \left(U_{A_0}\right)^L$, we have

$$U_{11} \cong V_{11}$$

say. If we consider A^L as the abstract group A acting on the faithful irreducible LA-module V_1, then $(V_1)_{A_0} = V_{11} \oplus \ldots \oplus V_{1t_1}$, and $A_0/\ker V_{11} = A_0/\ker U_{11} = A_0/\ker U_1 \cong B$. Hence $B^L \prec A^L$.

Conversely, suppose that $B^L \prec A^L$. We again consider A^L as A acting on V_1. Then there exists $A_0 \leq A$ such that $(V_1)_{A_0} = V_{11} \oplus \ldots \oplus V_{1t}$ where the V_{1j} are irreducible LA_0-modules and $A_0/\ker V_{11} \cong B$. As in above, we get $V_{11} \cong U_{11}$ say, and so $A_0/\ker U_1 = A_0/\ker U_{11} = A_0/\ker V_{11} \cong B$. Hence $B^K \prec A^K$. //

As in 1.2 we say that a class $\underline{\underline{X}}^E$ of (isomorphism classes) of irreducible linear groups over a field E is *closed* if it contains every irreducible linear factor of every linear group in $\underline{\underline{X}}^E$. The (set-theoretic) union and intersection of such closed classes are again clearly closed.

3.1.3 THEOREM. *There is a one-to-one correspondence from the closed classes of irreducible linear groups over K belonging to $\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_{q^n}$ onto the closed classes of irreducible linear groups over L belonging to $\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_{q^n}$.*

Proof. Let $\underline{\underline{X}}^K = \left\{A^K : A \in \underline{\underline{N}}_2 \wedge \underline{\underline{B}}_{q^n}\right\}$. Consider the class

$$\underline{\underline{X}}^L = \{A^L : A^K \in \underline{\underline{X}}^K\} .$$

By Lemma 3.1.2, $\underline{\underline{X}}^L$ is closed. It is clear that $\underline{\underline{X}}^K \leftrightarrow \underline{\underline{X}}^L$ gives the required correspondence. //

3.2 Linear groups over a splitting field.

In the section, A, B, C, D will always denote irreducible linear groups over the splitting field L (of the preceding section) belonging to $\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_{q^n}$. For simplicity we have omitted the superscript L. A closer analysis of the relation of being a linear factor is required before a classification of closed classes could be given.

This analysis will be undertaken here.

3.2.1 THEOREM. *$C \prec B$ and $B \prec A$ implies that $C \prec A$.*

Proof. Let U be a faithful irreducible LA-module. There exists $A_0 \leq A$ such that $U_{A_0} = U_1 \oplus \ldots \oplus U_r$, where the U_r are irreducible LA_0-modules and $A_0/\ker U_1 \cong B$. Write $A_0/\ker U_1 = \overline{A}_0$. Then U_1 is a faithful irreducible $L\overline{A}_0$-module, and there exists $\overline{A}_1 \leq \overline{A}_0$ with $\ker U_1 \leq A_1 \leq A_0$ such that

$$(U_1)_{\overline{A}_1} = U_{11} \oplus \ldots \oplus U_{1s},$$

where the U_{1j} are irreducible $L\overline{A}_1$-modules, and $\overline{A}_1/\ker U_{11} \cong C$. Let $\ker U_{11} = M_1/\ker U_1$, so that $A_1/M_1 \cong C$.

Now U_1 is an irreducible LA_0-module. Hence

$$(U_1)_{A_1} = V_1 \oplus \ldots \oplus V_t,$$

where the V_i are irreducible LA_1-modules, and

$$\bigcap_{i=1}^{t} \ker V_i = \ker (U_1)_{A_1} = A_1 \cap \ker U_1 = \ker U_1.$$

For each $1 \leq i \leq t$, define the action of $\overline{A}_1$ on V_i by

$$v\overline{x} = vx \quad \text{for all } v \in V_i, \ x \in A_1.$$

This is well-defined since $\ker U_1 \leq \ker V_i$. Hence V_i is an $L\overline{A}_1$-module. It is moreover irreducible. For if W is an $L\overline{A}_1$-submodule of V_i, then W is also an LA_1-submodule.

Thus considered as $L\overline{A}_1$-modules, we have

$$U_{11} \oplus \ldots \oplus U_{1s} = V_1 \oplus \ldots \oplus V_t.$$

Therefore $U_{11} \cong V_1$ say. As an $L\overline{A}_1$-module, the kernel of V_1 is $\ker V_1/\ker U_1$. Hence $M_1/\ker U_1 = \ker V_1/\ker U_1$, and so $M_1 = \ker V_1$. We then have, as LA_1-modules,

$$U_{A_1} = \left(U_{A_0}\right)_{A_1} = (U_1)_{A_1} \oplus \ldots \oplus (U_r)_{A_1}$$
$$= V_1 \oplus \ldots \oplus V_t \oplus \ldots ,$$

where $A_1/\ker V_1 = A_1/M_1 \cong C$. Hence $C \prec A$. //

We need the following preliminary results.

3.2.2 LEMMA. *Let U and V be vector spaces over a field F and let a and b be non-singular linear transformations of U and V respectively such that $a \otimes b = I$. Then $a = \lambda I$, $b = \lambda^{-1} I$ for some $0 \neq \lambda \in F$, where I denotes the identity transformation.*

Proof. Fix some bases of U and V, and represent a and b as the matrices (a_{ij}) and (b_{kl}) respectively. By a suitable choice of basis for $U \otimes_F V$, the matrix of $a \otimes b$ may be written in the form

$$\begin{pmatrix} a_{11}b & a_{12}b & \ldots & a_{1r}b \\ a_{21}b & a_{22}b & \ldots & a_{2r}b \\ \vdots & \vdots & & \vdots \\ a_{r1}b & a_{r2}b & \ldots & a_{rr}b \end{pmatrix}$$

where the $a_{ij}b$ are $s \times s$ block matrices. Hence

$$a_{ij}b = I_s \delta_{ij} , \quad i, j = 1, \ldots, r ,$$

where I_s is the $s \times s$ identity matrix, and δ_{ij} is the Kronecker delta. Since b is non-singular, we have $a_{ii} \neq 0$, $a_{ij} = 0$ if $i \neq j$ for $i, j = 1, \ldots, r$. For any fixed $1 \leq i \leq r$, $a_{ii}b = I_s$ implies that

$$a_{ii}b_{kl} = \delta_{kl} , \quad k, l = 1, \ldots, s .$$

This holds for any i, and hence $b_{11} = b_{22} = \ldots = b_{ss} = \lambda^{-1}$, $a_{11} = a_{22} = \ldots = a_{rr} = \lambda \neq 0$. In other words, $a = \lambda I_r$, $b = \lambda^{-1} I_s$. //

3.2.3 LEMMA. *Let R, S, T, RT and ST be subgroups of a group G satisfying the following conditions: $S \lhd R$, $ST \lhd RT$, $R \cap T \leq S$*

and $R \leq N_G(T)$. *Then* $R/S \cong RT/ST$.

Proof. Consider the following mapping

$$\varphi : RT \to R/S ,$$

$$xy \mapsto xS \quad \text{for all} \quad x \in R , \; y \in T .$$

Since $R \cap T \leq S$, φ is well-defined. We verify that φ is a homomorphism: for all $x_1, x_2 \in R$, $y_1, y_2 \in T$,

$$\begin{aligned}((x_1y_1)(x_2y_2))\varphi &= \left(x_1x_2 . y_1^{x_2}y_2\right)\varphi \\ &= (x_1x_2)S \text{ , since } R \leq N_G(T) , \\ &= x_1S . x_2S = (x_1y_1)\varphi . (x_2y_2)\varphi .\end{aligned}$$

Clearly φ is onto and $ST \leq \ker \varphi$. Conversely if $xy \in \ker \varphi$ for some $x \in R$, $y \in T$, then $xS = 1$ and so $x \in S$. Hence $\ker \varphi = ST$ and $RT/ST \cong R/S$. //

3.2.4 LEMMA. *Let* U *and* V *be faithful irreducible* LA- *and* LB-*modules respectively. Then the outer tensor product* $U \# V$ *is a faithful irreducible* $L(AB)$-*module where* AB *denotes the central product of* A *and* B *with cyclic centre.*

Proof. We may assume that $Z(A)$ is identified with a subgroup of $Z(B)$ so that the central product of A and B with cyclic centre may be written in the form $G = A \times B/N$, where $N = \{(z^{-1}, z) : z \in Z(A)\}$. By 2.1, Chapter 3, Gorenstein [9], we may suppose that $uz = \lambda u$, $vz = \lambda v$ for all $u \in U$, $v \in V$, $z \in Z(A)$ and some $0 \neq \lambda \in L$. Moreover $U \# V$ is an irreducible $L(A \times B)$-module by 7.1, Chapter 3, Gorenstein [9]. Clearly $N \leq \ker U \# V$. Conversely if $(a, b) \in \ker U \# V$, then $a \otimes b = 1$ and so $a = \mu I$, $b = \mu^{-1} I$ for some $0 \neq \mu \in L$, by Lemma 3.2.2. Hence $a \in Z(A)$ and $b = a^{-1}$, and so $(a, b) \in N$. It follows that $U \# V$ is a faithful irreducible LG-module. //

3.2.5 LEMMA. *Let* U *be a faithful irreducible* LA-*module. Suppose that* $A_0 \leq A$ *and* $U_{A_0} = U_1 \oplus \ldots \oplus U_r$ *where the* U_i *are irreducible* LA_0-*modules. Then* $Z(A) \cap \ker U_i = 1$, $i = 1, \ldots, r$.

Proof. Let $x \in Z(A) \cap \ker U_i$. Define

$$U_0 = \{u \in U : ux = u\} .$$

Then U_0 is an LA-module. For if $a \in A$, then $(ua)x = (ux)a = ua$ implies that $ua \in U_0$. Since U is irreducible, either $U_0 = 0$ or $U_0 = U$. But $U_i \neq 0$. Hence $U_0 = U$; that is, $x \in \ker U = 1$. //

We can now prove the following interesting result.

3.2.6 THEOREM. *$C \prec A$ and $D \prec B$ implies that $CD \prec AB$, where AB, CD denote central products with cyclic centres.*

Proof. Let U and V be faithful irreducible LA- and LB-modules respectively. By Lemma 3.2.4, $W = U \# V$ is a faithful irreducible LG-module, where $G = A \times B/N$ with $N = \{(z^{-1}, z) : z \in Z(A)\}$. (Without loss of generality, we can identify $Z(A)$ with a subgroup of $Z(B)$.)

Now there exist $A_0 \leq A$ and $B_0 \leq B$ such that $U_{A_0} = U_1 \oplus \ldots \oplus U_r$, $V_{B_0} = V_1 \oplus \ldots \oplus V_s$, where the U_i and V_j are irreducible LA_0- and LB_0-modules respectively, and $A_0/\ker U_1 \cong C$, $B_0/\ker V_1 \cong D$.

We claim that

$$Z(A_0/\ker U_1) = Z(A_0)\ker U_1/\ker U_1 ,$$

$$Z(B_0/\ker V_1) = Z(B_0)\ker V_1/\ker V_1 .$$

For let $\bar{x}_0 \in Z(A_0/\ker U_1)$ with $x_0 \in A_0$. Then $[\bar{x}_0, \bar{a}] = 1$ for all $a \in A_0$ implies that $[x, a] \in \ker U_1 \cap Z(A) = 1$ by Lemma 3.2.5. Similarly for $Z(B_0/\ker V_1)$. Hence we have

$$Z(A_0/\ker U_1) = \langle \bar{x} \rangle , \quad Z(B_0/\ker V_1) = \langle \bar{y} \rangle$$

for some $x \in Z(A_0)$, $y \in Z(B_0)$. By 2.1, Chapter 3, Gorenstein [9],

$$u\bar{x} = \lambda u , \quad v\bar{y} = \mu v$$

for all $u \in U_1$, $v \in V_1$ and some $0 \neq \lambda$, $\mu \in L$. Without loss of generality, assume that $|\bar{x}| = q^k$, $|\bar{y}| = q^l$, $k \leq l$. Then λ and μ are q^k-th and q^l-th roots of unity respectively, and we may

suppose $\lambda = \mu^{q^{l-k}}$. Put $x_1 = x$, $y_1 = y^{q^{l-k}}$, so that $\bar{x}_1 \mapsto \bar{y}_1$ is a monomorphism of $\langle \bar{x} \rangle$ into $\langle \bar{y} \rangle$. Define $N_0 = \langle (x_1^{-1}, y_1) \rangle$ and $\bar{N}_0 = \langle (\bar{x}_1^{-1}, \bar{y}_1) \rangle$. Note also that

$$Z(A_0) \leq \langle x, \ker U_1 \rangle , \quad Z(B_0) = \langle y, \ker V_1 \rangle .$$

Let us first consider W as an irreducible $L(A \times B)$-module so that in the decomposition

$$\begin{aligned} W_{A_0 \times B_0} &\cong U_{A_0} \# V_{B_0} \\ &\cong (U_1 \# V_1) \oplus \ldots \oplus (U_r \# V_s) , \end{aligned}$$

$U_1 \# V_1$ is an irreducible $L(A \times B)$-module and has kernel $N_0 N_1$, where $N_1 = \ker U_1 \times \ker V_1$.

We can also consider W as a faithful irreducible LG-module. Put $G_0 = (A_0 \times B_0)N/N$; then in the decomposition $W_{G_0} = (U_1 \# V_1) \oplus \ldots$, $U_1 \# V_1$ is an irreducible LG_0-module and has kernel $K_0 = N_0 N_1 N/N$. Moreover

$$\begin{aligned} G_0/K_0 &\cong (A_0 \times B_0)N/N_0 N_1 N \\ &\cong (A_0 \times B_0)/N_0 N_1 \quad \text{by Lemma 3.2.3,} \\ &\cong (A_0 \times B_0/N_1)/(N_0 N_1/N_1) \\ &\cong \bar{A}_0 \times \bar{B}_0/\bar{N}_0 , \end{aligned}$$

where $\bar{A}_0 = A_0/\ker U_1$, $\bar{B}_0 = B_0/\ker V_1$. But $\bar{A}_0 \times \bar{B}_0/\bar{N}_0$ is the central product CD. Hence $CD \prec AB$. //

The next lemma is useful.

3.2.7 LEMMA. *Let G be a monolithic group and let $N_i \lhd G$ such that $\bigcap_{i \in I} N_i = 1$ for some index set I. Then $N_i = 1$ for some $i \in I$.*

Proof. Let $1 \neq N$ be the monolith of G. Then $N_i \geq N$ if $N_i \neq 1$. So if $N_i \neq 1$ for all $i \in I$, then $\bigcap_{i \in I} N_i \geq N \neq 1$, a contradiction. Hence $N_i = 1$ for some $i \in I$. //

We then have

3.2.8 LEMMA. *Let* $A_0 \leq A$ *such that* A_0 *has cyclic centre. Then* A_0 *is an irreducible linear group and* $A_0 \prec A$.

Proof. Let U be a faithful irreducible LA-module. Then

$$U_{A_0} = U_1 \oplus \ldots \oplus U_r$$

where the U_i are irreducible LA_0-modules and $\bigcap_{i=1}^{r} \ker U_i = 1$. Clearly A_0 is monolithic and $\ker U_i \lhd A_0$, $i = 1, \ldots, r$. Hence from Lemma 3.2.7, $\ker U_j = 1$ for some $1 \leq j \leq r$, and so U_j is a faithful irreducible LA_0-module and $A_0 \prec A$. //

A subgroup of A does not necessarily determine a linear factor of A uniquely. But we can give the following sufficient condition.

3.2.9 THEOREM. *If* $A_0 \lhd A$, *then* A_0 *uniquely determines a linear factor of* A .

Proof. Let U be a faithful irreducible LA-module. Then by Clifford's Theorem, we have

$$U_{A_0} = U_1 \oplus \ldots \oplus U_r ,$$

where the U_i are irreducible LA_0-modules and are conjugates of each other.

First we show that $\ker U_1^{(a)} = \ker (U_1)^{a^{-1}}$ where $U_1^{(a)}$, $a \in A$, is a conjugate of U_1 . For let $x \in \ker U_1^{(a)}$; then for all $u \in U_1$, $u = u \circ x = u(a^{-1}xa)$ where $\circ$ denotes the action of A_0 on $U_1^{(a)}$. Hence $a^{-1}xa \in \ker U_1$, or $x \in (\ker U_1)^{a^{-1}}$. Conversely $(\ker U_1)^{a^{-1}} \leq \ker U_1^{(a)}$.

Next we show that for all $1 \leq i$, $j \leq r$, $A_0/\ker U_i \cong A_0/\ker U_j$. Now U_j is a conjugate of U_i ; that is, $U_j = U_i^{(a)}$ for some

$a \in A$. It has been shown above that $\ker U_i = \ker(U_j)^a$. The mapping,

$$\theta : A_0 \to A_0/(\ker U_j)^a$$
$$x \mapsto x^a(\ker U_j)^a ,$$

is an epimorphism with $\ker \theta = \ker U_j$. Therefore $A_0/\ker U_j \cong A_0/(\ker U_j)^a = A_0/\ker U_i$. In other words, each U_i gives rise to only one and the same irreducible linear group. //

There is an interesting connection between the relation of being a linear factor and the numbers $\rho_i(A)$ defined in 2.3.

3.2.10 THEOREM. *If* $B \prec A$, *then* $\rho_i(B) \le \rho_i(A)$, $i \ge 0$.

Proof. Since $B \prec A$, there exist $A_0 \le A$ and $N \lhd A_0$ such that $A_0/N \cong B$ and $N \cap Z(A) = 1$ (Lemma 3.2.5). In particular, $N \cap A_0' = 1$ and hence $Z(A_0/N) = Z(A_0)N/N$. We have

$$\begin{aligned}
\Omega^i(B/Z(B)) &= \Omega^i(B)Z(B)/Z(B) \\
&\cong \Omega^i(A_0/N)Z(A_0/N)/Z(A_0/N) \\
&= \frac{\Omega^i(A_0)Z(A_0)N/N}{Z(A_0)N/N} \\
&\cong \Omega^i(A_0)Z(A_0)N/Z(A_0)N \\
&\cong \Omega^i(A_0)/\Omega^i(A_0)\cap Z(A_0)N \\
&\cong \Omega^i(A_0)Z(A)/\left(\Omega^i(A_0)\cap Z(A_0)N\right)Z(A) ,
\end{aligned}$$

by Lemma 3.2.3. Write

$$\overline{A} = \Omega^i(A/Z(A)) \quad , \quad \overline{B} = \Omega^i(B/Z(B)) \quad ,$$
$$\overline{A}_0 = \Omega^i(A_0)Z(A)/Z(A) \quad , \quad \overline{N}_0 = \left(\Omega^i(A_0)\cap Z(A_0)N\right)Z(A)/Z(A) .$$

Then $\overline{B} \cong \overline{A}_0/\overline{N}_0$ and $\overline{A}_0 \le \overline{A}$. Since $\overline{A}$ is an abelian q-group, $d(\overline{B}) = d(\overline{A}_0/\overline{N}_0) \le d(\overline{A}_0) \le d(\overline{A})$. //

We now give some easy examples of linear factors.

3.2.11 LEMMA.

(i) $Q(n, 0) \prec Q(n, 1) \prec \ldots \prec Q(n, n-1) \prec Q(n, n)$.

(ii) $Q(n-1, r-1) \prec Q(n, r)$, $0 < r < n$.

Proof. *(i)* Obviously $Q(n, 0) \prec Q(n, 1)$. Suppose that $0 < r \leq n$. Let $A = Q(n, r) = \langle a, b \rangle$ and let U be a faithful irreducible LA-module. Put $A_0 = \langle a, b^q \rangle$. Then in the decomposition

$$U_{A_0} = U_1 \oplus \ldots \oplus U_s$$

into irreducible LA_0-modules, there is some U_i , $1 \leq i \leq s$, such that $a^{q^{n-1}} \notin \ker U_i$. Also $A_0' \cap \ker U_i = 1$ by Lemma 3.2.5. Hence $A_0/\ker U_i$ has exponent q^n , cyclic centre and derived group of exponent q^{r-1} . Therefore $A_0/\ker U_i \tilde{=} Q(n, r-1)$ and so $Q(n, r-1) \prec Q(n, r)$.

Let $A = Q(n, r) = \langle a, b \rangle$, $0 < r < n$. Take $A_0 = \langle a^q, b \rangle$. By the same argument as in *(i)*, there is an irreducible LA_0-module U_i such that $A_0/\ker U_i$ has exponent q^{n-1} , cyclic centre and derived group of exponent q^{r-1} so that $A_0/\ker U_i \tilde{=} Q(n-1, r-1)$. //

We have gathered enough information on linear factors to allow us to give a classification of the closed classes of irredicuble linear groups in $\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_{q^n}$ when q is an odd prime. This is done in an inductive process. Though essentially qualitative in description, it enables us to prove some interesting results.

3.3 A classification of the closed classes

In this section, q is an odd prime and n is a fixed integer greater than 1 . We denote by $\underline{\underline{O}}_i$ the class of all the irreducible linear groups in $\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_{q^i}$ for $1 \leq i \leq n$. To simplify the

terminological presentation of results, we adopt the convention that an empty class is closed. The symbols $\underline{\underline{X}}$, $\underline{\underline{Y}}$, $\underline{\underline{Z}}$ will always denote closed classes in $\underline{\underline{Q}}_n$, possibly with subscripts or superscripts, and X, Y, Z will denote irreducible linear groups in $\underline{\underline{Q}}_n$. For any two linear groups X and Y, we denote by XY the central product of X and Y with cyclic centre. Inclusion between two closed classes will be denoted by $\leq$.

For every closed class $\underline{\underline{X}} \leq \underline{\underline{Q}}_n$, we define the following classes $\underline{\underline{X}}_i$, $\underline{\underline{X}}^j$ in $\underline{\underline{Q}}_{n-1}$, $i = 0, 1, \ldots, n-1$, $j = 0, 1, \ldots$

$$\underline{\underline{X}}_i = \{X \in \underline{\underline{Q}}_{n-1} : Q(n, i)X \in \underline{\underline{X}}\}, \quad i = 0, 1, \ldots, n-1,$$

$$\underline{\underline{X}}^j = \left\{X \in \underline{\underline{Q}}_{n-1} : Q(n, n)^j X \in \underline{\underline{X}}\right\}, \quad j = 0, 1, \ldots,$$

where $Q(n, n)^0 = 1$. Note that some of them may be empty.

3.3.1 LEMMA. *The classes* $\underline{\underline{X}}_i$, $\underline{\underline{X}}^j$ *are closed.*

Proof. We may suppose that $\underline{\underline{X}}_i$ is non-empty. Let $Y \prec X \in \underline{\underline{X}}_i$. Then $Q(n, i)Y \prec Q(n, i)X$ by Theorem 3.2.6. Since $Q(n, i)X \in \underline{\underline{X}}$ by definition, and $\underline{\underline{X}}$ is closed, it follows that $Q(n, i)Y \in \underline{\underline{X}}$ and so $Y \in \underline{\underline{X}}_i$. Hence $\underline{\underline{X}}_i$ is closed. Similarly for $\underline{\underline{X}}^j$. //

3.3.2 LEMMA.

$$\underline{\underline{X}}^0 \geq \underline{\underline{X}}_0 \geq \underline{\underline{X}}_1 \geq \ldots \geq \underline{\underline{X}}_{n-1},$$

$$\underline{\underline{X}}^0 \geq \underline{\underline{X}}^1 \geq \ldots \geq \underline{\underline{X}}^j \geq \underline{\underline{X}}^{j+1} \geq \ldots.$$

Proof. Let $X \in \underline{\underline{X}}_0$. Then by Theorem 3.2.8, $X \prec Q(n, 0)X \in \underline{\underline{X}}$ and hence $X \in \underline{\underline{X}}$, that is, $X \in \underline{\underline{X}}^0$. Therefore $\underline{\underline{X}}_0 \leq \underline{\underline{X}}^0$. Next suppose that $0 < i < n$ and $X \in \underline{\underline{X}}_i$. Then from Lemma 3.2.11 and Theorem 3.2.6, we have $Q(n, i-1)X \prec Q(n, i)X \in \underline{\underline{X}}$ and so $Q(n, i-1)X \in \underline{\underline{X}}$, that is, $X \in \underline{\underline{X}}_{i-1}$. Hence $\underline{\underline{X}}_i \leq \underline{\underline{X}}_{i-1}$.

Finally let $X \in \underline{\underline{X}}^j$, $j > 0$. Then

$Q(n, n)^{j-1}X \prec Q(n, n)^{j}X \in \underline{\underline{X}}$ and hence $Q(n, n)^{j-1}X \in \underline{\underline{X}}$; so $X \in \underline{\underline{X}}^{j-1}$. The second chain of inclusions is thus proved. //

In the rest of the discussion in this section, Theorems 3.2.1, 3.2.6, and 3.2.8 and Lemma 3.2.11 will be frequently used. For the sake of brevity, we shall omit references to them. It will be clear from the context which one of them has been used.

We define the *index* of a *non-empty* closed class $\underline{\underline{X}}$ to be the number $\sup\{j : Q(n, n)^{j} \in \underline{\underline{X}}\}$, which may be infinite. We set the *index* of an *empty* class to be -1 .

3.3.3 THEOREM. *$\underline{\underline{X}}$ is properly contained in $\underline{\underline{O}}_n$ if and only if the index of $\underline{\underline{X}}$ is finite.*

Proof. Sufficiency is easy. The necessity part follows immediately if we can show that every irreducible linear group $X \in \underline{\underline{O}}_n$ is a factor of $Q(n, n)^{j}$ for some $j > 0$. Let $0 \leq s \leq m \leq n$. Then

$$Q(m, s) \prec Q(m, 0)Q(s, s) \prec Q(n, 0)Q(n, s) \prec Q(n, n)^{2} .$$

Since X is a central product of the $Q(m, s)$, it follows that $X \prec Q(n, n)^{j}$ for some sufficiently large integer $j > 0$. //

3.3.4 COROLLARY. *If $\underline{\underline{X}}$ is properly contained in $\underline{\underline{O}}_n$, then $\underline{\underline{X}}^{j}$ is empty for all $j >$ index of $\underline{\underline{X}}$.*

Proof. The index of $\underline{\underline{X}}$ is finite by the preceding theorem. Suppose $\underline{\underline{X}}^{j}$ is non-empty for some $j >$ index of $\underline{\underline{X}}$. Then for some $X \in \underline{\underline{O}}_{n-1}$, $Q(n, n)^{j}X \in \underline{\underline{X}}$ and so $Q(n, n)^{j} \in \underline{\underline{X}}$; whence $j \leq$ index of $\underline{\underline{X}}$, contradicting the choice of j . //

Evidently $\underline{\underline{X}}$ determines a sequence $(\underline{\underline{X}}) = \left(\underline{\underline{X}}_0, \underline{\underline{X}}_1, \ldots, \underline{\underline{X}}_{n-1}, \underline{\underline{X}}^{0}, \underline{\underline{X}}^{1}, \ldots\right)$ of closed classes in $\underline{\underline{O}}_{n-1}$, but an arbitrary sequence of closed classes in $\underline{\underline{O}}_{n-1}$ does not necessarily arise in this way. The classes $\underline{\underline{X}}_i$, $\underline{\underline{X}}^{j}$ satisfy certain properties which distinguish the sequence $(\underline{\underline{X}})$ from an arbitrary

sequence. This leads us to the next definition.

A sequence $(\underline{\underline{Y}}) = (\underline{\underline{Y}}_0, \underline{\underline{Y}}_1, \ldots, \underline{\underline{Y}}_n, \underline{\underline{Y}}_{n+1}, \ldots)$ of closed classes $\underline{\underline{Y}}_i$ in $\underline{\underline{Q}}_{n-1}$ is called a *closed sequence* of $\underline{\underline{Q}}_{n-1}$ if the following conditions are satisfied:

(i) if $0 \leq k \leq i < n$, $Z \in \underline{\underline{Q}}_{n-1}$, $Y \in \underline{\underline{Y}}_i$ and $Q(n, k)Z \prec Q(n, i)Y$, then $Z \in \underline{\underline{Y}}_k$;

(ii) if $0 \leq i < n$, $Z \in \underline{\underline{Q}}_{n-1}$, $Y \in \underline{\underline{Y}}_i$ and $Z \prec Q(n, i)Y$, then $Z \in \underline{\underline{Y}}_n$;

(iii) if $0 \leq l \leq j$, $Z \in \underline{\underline{Q}}_{n-1}$, $Y \in \underline{\underline{Y}}_{n+j}$ and $Q(n, n)^l Z \prec Q(n, n)^j Y$, then $Z \in \underline{\underline{Y}}_{n+l}$,

(iv) if $0 \leq i < n$, $j > 0$, $Z \in \underline{\underline{Q}}_{n-1}$, $Y \in \underline{\underline{Y}}_{n+j}$ and $Q(n, i)Z \prec Q(n, n)^j Y$, then $Z \in \underline{\underline{Y}}_i$.

We order the closed sequences of $\underline{\underline{Q}}_{n-1}$ as follows: $(\underline{\underline{Y}}) \leq (\underline{\underline{Z}})$ if $\underline{\underline{Y}}_i \leq \underline{\underline{Z}}_i$, $i = 0, 1, \ldots$. We also define the union and intersection of closed sequences by

$$(\underline{\underline{Y}}) \cup (\underline{\underline{Z}}) = (\underline{\underline{Y}}_0 \cup \underline{\underline{Z}}_0, \underline{\underline{Y}}_1 \cup \underline{\underline{Z}}_1, \ldots),$$

$$(\underline{\underline{Y}}) \cap (\underline{\underline{Z}}) = (\underline{\underline{Y}}_0 \cap \underline{\underline{Z}}_0, \underline{\underline{Y}}_1 \cap \underline{\underline{Z}}_1, \ldots).$$

The next lemma shows that these definitions are meaningful.

3.3.5 LEMMA. *If* $(\underline{\underline{Y}})$ *and* $(\underline{\underline{Z}})$ *are closed sequences of* $\underline{\underline{Q}}_{n-1}$, *then* $(\underline{\underline{Y}}) \cup (\underline{\underline{Z}})$ *and* $(\underline{\underline{Y}}) \cap (\underline{\underline{Z}})$ *are also closed sequences of* $\underline{\underline{Q}}_{n-1}$.

Proof. Let $\underline{\underline{X}}_i = \underline{\underline{Y}}_i \cup \underline{\underline{Z}}_i$, $i = 0, 1, \ldots$. Clearly the $\underline{\underline{X}}_i$ are closed. We have to verify that they satisfy the required conditions. Firstly let $0 \leq k \leq i < n$, $Z \in \underline{\underline{Q}}_{n-1}$, $Y \in \underline{\underline{X}}_i$ and $Q(n, k)Z \prec Q(n, i)Y$. Since Y belongs to $\underline{\underline{Y}}_i$ or $\underline{\underline{Z}}_i$, and $(\underline{\underline{Y}})$, $(\underline{\underline{Z}})$ are closed sequences, it follows that Z belongs to $\underline{\underline{Y}}_k$ or $\underline{\underline{Z}}_k$, that is, $Z \in \underline{\underline{X}}_i$. The remaining three conditions are similarly verified. Likewise for $\underline{\underline{Y}}_i \cap \underline{\underline{Z}}_i$. //

To see that closed sequences do exist and arise in a natural way, we give the following two lemmas.

3.3.6 LEMMA. *For any closed class* $\underline{\underline{X}} \leq \underline{\underline{Q}}_n$, *the sequence*

$$(\underline{\underline{X}}) = \left(\underline{\underline{X}}_0, \ldots, \underline{\underline{X}}_{n-1}, \underline{\underline{X}}^0, \underline{\underline{X}}^1, \ldots\right)$$

is a closed sequence of $\underline{\underline{Q}}_{n-1}$.

Proof. If we rewrite $\underline{\underline{X}}^j = \underline{\underline{X}}_{n+j}$, $j = 0, 1, \ldots$, we can easily check that the required conditions for closed sequences are satisfied by the $\underline{\underline{X}}_i$, $i = 0, 1, \ldots$. //

3.3.7 LEMMA. *For any closed sequence* $(\underline{\underline{Y}})$ *of* $\underline{\underline{Q}}_{n-1}$,

$$\underline{\underline{Y}}_n \geq \underline{\underline{Y}}_0 \geq \underline{\underline{Y}}_1 \geq \ldots \geq \underline{\underline{Y}}_{n-1} ,$$

$$\underline{\underline{Y}}_n \geq \underline{\underline{Y}}_{n+1} \geq \underline{\underline{Y}}_{n+2} \geq \ldots .$$

Proof. The proof is straightforward. To illustrate, we show that for $0 < i < n$, $\underline{\underline{Y}}_i \leq \underline{\underline{Y}}_{i-1}$. Suppose $Y \in \underline{\underline{Y}}_i$; then since $Q(n, i\text{-}1)Y \prec Q(n, i)Y$, we have, by the definition of a closed sequence, $Y \in \underline{\underline{Y}}_{i-1}$. //

The classification of closed classes in $\underline{\underline{Q}}_1$ is almost trivial. Under the operations of (set-theoretic) union and intersection, the closed classes in $\underline{\underline{Q}}_1$ form a chain lattice by virtue of the fact that

$$1 \prec Q(1, 0) \prec Q(1, 1) \prec Q(1, 1)^2 \prec \ldots .$$

We reduce the problem of the classification of closed classes in $\underline{\underline{Q}}_n$ to that in $\underline{\underline{Q}}_{n-1}$. Thus a complete knowledge of closed classes in $\underline{\underline{Q}}_1$ classifies closed classes in $\underline{\underline{Q}}_n$ by an inductive process. In fact, we will show that the closed classes in $\underline{\underline{Q}}_n$ are determined by the closed sequences of $\underline{\underline{Q}}_{n-1}$.

3.3.8 THEOREM. *There is a one-to-one correspondence from the closed classes of* $\underline{\underline{Q}}_n$ *onto the closed sequences of* $\underline{\underline{Q}}_{n-1}$.

A closed class $\underline{\underline{X}}$ is properly contained in $\underline{\underline{Q}}_n$ if and only if

the corresponding closed sequence $(\underline{\underline{X}})$ has only finitely many non-empty closed classes.

Let $\underline{\underline{X}} \leftrightarrow (\underline{\underline{X}})$ and $\underline{\underline{Y}} \leftrightarrow (\underline{\underline{Y}})$. Then

(i) $\underline{\underline{X}} \cup \underline{\underline{Y}} \leftrightarrow (\underline{\underline{X}}) \cup (\underline{\underline{Y}})$,

(ii) $\underline{\underline{X}} \cap \underline{\underline{Y}} \leftrightarrow (\underline{\underline{X}}) \cap (\underline{\underline{Y}})$,

(iii) $\underline{\underline{X}} \leq \underline{\underline{Y}}$ if and only if $(\underline{\underline{X}}) \leq (\underline{\underline{Y}})$.

Proof. For every $\underline{\underline{X}} \leq \underline{\underline{O}}_n$, the sequence $(\underline{\underline{X}}) = \left(\underline{\underline{X}}_0, \ldots, \underline{\underline{X}}_{n-1}, \underline{\underline{X}}^0, \underline{\underline{X}}^1, \ldots\right)$ is a closed sequence of $\underline{\underline{O}}_{n-1}$ by Lemma 3.3.6. Conversely, given any closed sequence $(\underline{\underline{Y}}) = (\underline{\underline{Y}}_0, \underline{\underline{Y}}_1, \ldots)$, let

$$\underline{\underline{S}}_i = \{Q(n, i)Y : Y \in \underline{\underline{Y}}_i\}, \quad i = 0, 1, \ldots, n-1,$$

$$\underline{\underline{S}}_{n+j} = \left\{Q(n, n)^j Y : Y \in \underline{\underline{Y}}_{n+j}\right\}, \quad j = 0, 1, \ldots.$$

Set $\underline{\underline{S}}_k$ to be the empty class if $\underline{\underline{Y}}_k$ is empty. Define

$$\underline{\underline{X}} = \left(\bigcup_{i=0}^{n-1} \underline{\underline{S}}_i\right) \cup \left(\bigcup_{j=0}^{\infty} \underline{\underline{S}}_{n+j}\right).$$

Then $\underline{\underline{X}}$ is a closed class since the properties of closed sequences ensure that every linear factor of $\underline{\underline{S}}_k$ belongs to some $\underline{\underline{S}}_l$. Now if we define the closed classes $\underline{\underline{X}}_i$, $\underline{\underline{X}}^j$ as usual, then it is easily seen that

$$\underline{\underline{X}}_i = \underline{\underline{Y}}_i, \quad i = 0, 1, \ldots, n-1,$$

$$\underline{\underline{X}}^j = \underline{\underline{Y}}_{n+j}, \quad j = 0, 1, \ldots.$$

To illustrate, we show that $\underline{\underline{X}}_i = \underline{\underline{Y}}_i$. Let $Y \in \underline{\underline{Y}}_i$; then by definition, $Q(n, i)Y \in \underline{\underline{X}}$ and so $Y \in \underline{\underline{X}}_i$. Conversely if $X \in \underline{\underline{X}}_i$, then $Q(n, i)X \in \underline{\underline{X}}$ and so $Q(n, i)X \in \underline{\underline{S}}_i$. Hence $Q(n, i)X \cong Q(n, i)Y$ for some $Y \in \underline{\underline{Y}}_i$, or $Q(n, i)X \prec Q(n, i)Y$. Since $(\underline{\underline{Y}})$ is a closed sequence, $X \in \underline{\underline{Y}}_i$. Hence $\underline{\underline{X}}_i = \underline{\underline{Y}}_i$.

Consider the following correspondence

$$\underline{\underline{X}} \leftrightarrow (\underline{\underline{X}}) = \left(\underline{\underline{X}}_0, \underline{\underline{X}}_1, \ldots, \underline{\underline{X}}_{n-1}, \underline{\underline{X}}^0, \underline{\underline{X}}^1, \ldots\right) .$$

It is clear that this is one-to-one. By the above remarks, this gives a one-to-one correspondence from the closed classes of $\underline{\underline{Q}}_n$ onto the closed sequences of $\underline{\underline{Q}}_{n-1}$.

If $\underline{\underline{X}} \neq \underline{\underline{Q}}_n$, then by Corollary 3.3.4, only finitely many of the $\underline{\underline{X}}^j$ are non-empty. Conversely, if $(\underline{\underline{X}})$ has only finitely many non-empty closed classes, then $\underline{\underline{X}}^j$ is empty for some $j \geq 0$ and so the index of $\underline{\underline{X}}$ is finite. Hence $\underline{\underline{X}}$ is properly contained in $\underline{\underline{Q}}_n$ by Theorem 3.3.3.

Write $\underline{\underline{Z}} = \underline{\underline{X}} \cup \underline{\underline{Y}}$. Evidently we have

$$\underline{\underline{Z}}_i = \underline{\underline{X}}_i \cup \underline{\underline{Y}}_i , \quad i = 0, 1, \ldots, n-1 ,$$

$$\underline{\underline{Z}}^j \quad \underline{\underline{X}}^j \cup \underline{\underline{Y}}^j , \quad j = 0, 1, \ldots .$$

Hence $\underline{\underline{Z}} \leftrightarrow (\underline{\underline{Z}}) = \left(\underline{\underline{Z}}_0, \ldots, \underline{\underline{Z}}_{n-1}, \underline{\underline{Z}}^0, \ldots\right) = (\underline{\underline{X}}) \cup (\underline{\underline{Y}})$. Similarly for $\underline{\underline{X}} \cap \underline{\underline{Y}}$. The last assertion follows from the fact that $\underline{\underline{X}} \leq \underline{\underline{Y}}$ if and only if $\underline{\underline{X}}_i \leq \underline{\underline{Y}}_i$, $\underline{\underline{X}}^j \leq \underline{\underline{Y}}^j$, $i = 0, 1, \ldots, n-1$, $j = 0, 1, \ldots$. //

As an application of the above theorem, we have

3.3.9 THEOREM. *The lattice of subvarieties of* $\underline{\underline{A}}_p\left(\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_{qn}\right)$ *containing* $\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_{qn}$ *is distributive.*

Proof. By Theorem 1.2.1 and Lemma 1.2.2, it is sufficient to show that the lattice of closed classes in $\underline{\underline{Q}}_n$ is distributive. We use induction on n. This is obviously true when $n = 1$ since $\underline{\underline{Q}}_1$ is a chain. So suppose that $n > 1$ and that the lattice of closed classes in $\underline{\underline{Q}}_{n-1}$ is distributive. Write

$$\underline{\underline{S}} = \underline{\underline{X}} \cap (\underline{\underline{Y}} \cup \underline{\underline{X}}) ,$$

$$\underline{\underline{T}} = (\underline{\underline{X}} \cap \underline{\underline{Y}}) \cup (\underline{\underline{X}} \cap \underline{\underline{Z}}) ,$$

where $\underline{\underline{X}}, \underline{\underline{Y}}, \underline{\underline{Z}} \leq \underline{\underline{Q}}_n$. By Theorem 3.3.8, we have

$$\underline{\underline{S}} \leftrightarrow (\underline{\underline{S}}) = \left(\underline{\underline{S}}_0, \ldots, \underline{\underline{S}}_{n-1}, \underline{\underline{S}}^0, \underline{\underline{S}}^1, \ldots\right) ,$$

$$\underline{\underline{T}} \leftrightarrow (\underline{\underline{T}}) = \left(\underline{\underline{T}}_0, \ldots, \underline{\underline{T}}_{n-1}, \underline{\underline{T}}^0, \underline{\underline{T}}^1, \ldots\right) ,$$

where

$$\underline{\underline{S}}_i = \underline{\underline{X}}_i \cap (\underline{\underline{Y}}_i \cup \underline{\underline{Z}}_i) , \quad i = 0, 1, \ldots, n-1 ,$$

$$\underline{\underline{S}}^j = \underline{\underline{X}}^j \cap (\underline{\underline{Y}}^j \cup \underline{\underline{Z}}^j) , \quad j = 0, 1, \ldots ,$$

$$\underline{\underline{T}}_i = (\underline{\underline{X}}_i \cap \underline{\underline{Y}}_i) \cup (\underline{\underline{X}}_i \cap \underline{\underline{Z}}_i) , \quad i = 0, 1, \ldots, n-1 ,$$

$$\underline{\underline{T}}^j = (\underline{\underline{X}}^j \cap \underline{\underline{Y}}^j) \cup (\underline{\underline{X}}^j \cap \underline{\underline{Z}}^j) , \quad j = 0, 1, \ldots .$$

Since the $\underline{\underline{X}}_i$, $\underline{\underline{X}}^j$, $\underline{\underline{Y}}_i$, $\underline{\underline{Y}}^j$ are in $\underline{\underline{Q}}_{n-1}$, we have by the induction hypothesis, $\underline{\underline{S}}_i = \underline{\underline{T}}_i$, $\underline{\underline{S}}^j = \underline{\underline{T}}^j$, $i = 0, 1, \ldots, n-1$, $j = 0, 1, \ldots$. Hence $(\underline{\underline{S}}) = (\underline{\underline{T}})$ and so $\underline{\underline{S}} = \underline{\underline{T}}$. //

We give another proof of a well-known theorem of Brady, Bryce and Cossey.

3.3.10 THEOREM (Brady, Bryce and Cossey [4]). *The subvarieties of* $\underline{\underline{A}}_p\left(\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_q n\right)$ *are finitely based for* q *odd.*

Proof. It is again sufficient to show that the closed classes in $\underline{\underline{Q}}_n$ satisfy the descending chain condition. Evidently this is true for $n = 1$ since $\underline{\underline{Q}}_1$ is a chain. So suppose that $n > 1$ and that the closed classes in $\underline{\underline{Q}}_{n-1}$ satisfy the descending chain condition. Let

$$\underline{\underline{X}}_1 \geq \ldots \geq \underline{\underline{X}}_k \geq \underline{\underline{X}}_{k+1} \geq \ldots$$

be a descending chain of closed classes in $\underline{\underline{Q}}$, and let the corresponding closed sequences of $\underline{\underline{Q}}_{n-1}$ be given by

$$(\underline{\underline{X}}_k) = \left(\underline{\underline{X}}_{k,0}, \ldots, \underline{\underline{X}}_{k,n-1}, \underline{\underline{X}}_k^0, \underline{\underline{X}}_k^1, \ldots\right) , \quad k = 1, 2, \ldots .$$

We then have the following descending chains in $\underline{\underline{Q}}_{n-1}$:

$$\underline{\underline{X}}_{1,i} \geq \ldots \geq \underline{\underline{X}}_{k,i} \geq \underline{\underline{X}}_{k+1,i} \geq \ldots , \quad i = 0, 1, \ldots, n-1 , \qquad (*)$$

$$\underline{\underline{X}}_1^j \geq \ldots \geq \underline{\underline{X}}_k^j \geq \underline{\underline{X}}_{k+1}^j \geq \ldots , \quad j = 0, 1, \ldots . \qquad (**)$$

Each chain in (*) terminates by the induction hypothesis and since there are only finitely many chains in (*), there exists $r > 0$ such that

$$\underline{\underline{X}}_{r,i} = \underline{\underline{X}}_{r+1,i} = \cdots , \quad i = 0, 1, \ldots, n-1 .$$

Now clearly, index of $\underline{\underline{X}}_1 \geq$ index of $\underline{\underline{X}}_2 \geq \cdots$. If the index of $\underline{\underline{X}}_k$ is infinite for all $k = 1, 2, \ldots$, then by Theorem 3.3.3, $\underline{\underline{X}}_k = \underline{\underline{O}}_n$ for all $k = 1, 2, \ldots$. So suppose l is the smallest positive integer for which the index of $\underline{\underline{X}}_l < \infty$, that is, index of $\underline{\underline{X}}_k \leq m =$ index of $\underline{\underline{X}}_l$ for all $k \geq l$. Consequently if $j > m$, $\underline{\underline{X}}_k^j$ is empty for all $k \geq l$ by Corollary 3.3.4. By hypothesis, the remaining chains in (**) also terminate, that is, for $j = 0, 1, \ldots, m$. Hence there exists $s > 0$ such that $\underline{\underline{X}}_s^j = \underline{\underline{X}}_{s+1}^j = \cdots$ for $j = 0, 1, \ldots, m$, and $\underline{\underline{X}}_k^j$ is empty for all $k \geq s$ and $j > m$. In other words,

$$\underline{\underline{X}}_s^j = \underline{\underline{X}}_{s+1}^j = \cdots , \quad j = 0, 1, \ldots .$$

Put $t = \max\{r, s\}$. Then $\underline{\underline{X}}_t = \underline{\underline{X}}_{t+1} = \cdots$. //

CHAPTER 4

SYMPLECTIC MODULES AND LINEAR AUTOMORPHISMS

The structure of alternating bilinear forms on vector spaces over a field is well-known: see, for example, Artin [1], Huppert [16] and Lang [18]. In 4.1, we study the structure of alternating bilinear forms on modules (not necessarily free) over Z_{q^α}, the ring of integers modulo q^α, where q is an odd prime. However, for our purposes, we do not need the full generality of the corresponding results in the case of vector spaces. We introduce the notion of a non-degenerate symplectic module U over Z_{q^α} and define, in the natural way, the group $Sp(U)$ of isometries of U. By a method analogous to that of Huppert [16], we calculate the order of $Sp(U)$ by enumerating the "hyperbolic pairs" of U.

In 4.2 we reduce the problem of calculating the order of lin aut G, the group of linear automorphisms of G where G is a finite q-group of class 2 with cyclic centre (q odd), to one of calculating the order of a certain subgroup of $Sp(U)$ for some non-degenerate symplectic module U over Z_{q^m}. This involves an elaborate enumeration of "quasi-hyperbolic pairs". The order of lin aut G will be needed in the next chapter.

Finally in 4.3, we give some extensions of certain results of Winter [26]. Though not essential to the development of the next chapter, they are of independent interest.

4.1 Symplectic modules over Z_{q^α}

Let us recall some terminologies on rings and modules. Let R be a commutative ring with unity, and U a unitary R-module. A finite set of elements of U, $\{u_1, \ldots, u_r\}$, is *linearly independent* (over R) if: $\xi_1 u_1 + \ldots + \xi_r u_r = 0$, where $\xi_i \in R$, implies that $\xi_i = 0$ for all $i = 1, \ldots, r$. Otherwise $\{u_1, \ldots, u_r\}$ is *linearly dependent*. A *basis* of U is a linearly independent set of generators for U. We will be concerned with finitely generated

modules only. U is *free* if and only if there is a basis of U. If $u_1, \ldots, u_r \in U$, then $\langle u_1, \ldots, u_r \rangle$ denotes the submodule generated by $u_1, \ldots, u_r$. An element of U is said to be a *torsion* element if $\xi u = 0$ for some $0 \neq \xi \in R$; otherwise u is *torsion-free*. An element ξ of R is *invertible* if $\xi\xi' = 1$ for some $\xi' \in R$.

An *R-bilinear form* on U is a map $f : U \times U \to R$ which satisfies the following conditions for all $u, v, w \in U$ and all $\xi \in R$:

$$f(u+v, w) = f(u, w) + f(v, w) ,$$

$$f(u, v+w) = f(u, v) + f(u, w) ,$$

$$f(\xi u, v) = \xi f(u, v) = f(u, \xi v) .$$

We say that f is an *alternating R-bilinear form* if $f(u, u) = 0$ for all $u \in U$. If f is alternating, it is easily verified that $f(u, v) = -f(v, u)$ for all $u, v \in U$. For simplicity, we write (u, v) for $f(u, v)$. If $u, v \in U$, then $u \perp v$ means that $(u, v) = 0$. Similarly, if X and Y are subsets of U, then $X \perp Y$ means that $(x, y) = 0$ for all $x \in X$ and all $y \in Y$. However, if V is a submodule of U, we write $V = V_1 \perp V_2$ to denote that $V = V_1 \oplus V_2$ and $V_1 \perp V_2$. For any subset S of U, we define

$$S^{\perp} = \{u \in U : (u, x) = 0 \text{ for all } x \in S\} .$$

We say that f, or $(\cdot, \cdot)$, is non-degenerate if $U^{\perp} = 0$.

In this section, we only consider the case when $R = Z_{q^\alpha}$. Since R is then finite, it follows that every basis of a finitely generated free R-module U has the same number of elements, which is called the *dimension* of U and is denoted by $\dim U$. We start off with the following observation.

4.1.1 LEMMA. *Let U be a free Z_{q^α}-module, and V a free Z_{q^α}-submodule of U. Then every Z_{q^α}-basis of V can be extended to a Z_{q^α}-basis of U.*

Proof. Let $\{u_1, \ldots, u_r\}$ be a basis of U, and $\{v_1, \ldots, v_s\}$

a basis of V. Now $v_1 = \xi_1 u_1 + \ldots + \xi_r u_r$ for some $\xi_i \in Z_{q^\alpha}$. Then ξ_j is invertible for some $1 \leq j \leq r$; otherwise $q^{\alpha-1} v_1 = 0$. We may assume that ξ_1 is invertible. Then

$$u_1 = \xi_1^{-1} v_1 - \xi_1^{-1}(\xi_2 u_2 + \ldots + \xi_r u_r) ,$$

and $\{v_1, u_2, \ldots, u_r\}$ is a linearly independent set. For if

$$\eta_1 v_1 + \eta_2 u_2 + \ldots + \eta_r u_r = 0 \quad \text{for some } \eta_i \in Z_{q^\alpha} ,$$

then $\xi_1\eta_1 u_1 + (\xi_2\eta_1+\eta_2)u_2 + \ldots + (\xi_r\eta_1+\eta_r)u_r = 0$, and hence $\xi_1\eta_1 = 0 = \xi_i\eta_1 + \eta_i$, $i = 2, \ldots, r$. So $\eta_i = 0$, $i = 1, \ldots, r$.

Since U is then generated by $\{v_1, u_2, \ldots, u_r\}$ we have $v_2 = \zeta_1 v_1 + \zeta_2 u_2 + \ldots + \zeta_r u_r$ for some $\zeta_i \in Z_{q^\alpha}$. We claim that ζ_j is invertible for some $2 \leq j \leq r$. If not, then $q^{\alpha-1} v_2 = q^{\alpha-1}\zeta_1 v_1$ and so $q^{\alpha-1} v_2 = 0$, which is impossible. We may assume that ζ_2 is invertible. It is easily checked that $\{v_1, v_2, u_3, \ldots, u_r\}$ is linearly independent and hence is a basis of U. In this way, we replace s elements of $\{u_1, \ldots, u_r\}$ by those of $\{v_1, \ldots, v_s\}$ to produce another basis of U. //

We now define the object under study. A finitely generated Z_{q^α}-module U is a *symplectic module* (over Z_{q^α}) if there is an alternating Z_{q^α}-bilinear form defined on U. If the bilinear form is non-degenerate, then U is said to be *non-degenerate*. The bilinear form is, of course, kept fixed once it is chosen. We will be mainly interested in non-degenerate symplectic modules. In particular, the free ones are easily characterized.

4.1.2 LEMMA. *Let U be a free non-degenerate symplectic module over Z_{q^α}. Then $U = \langle u_1, v_1 \rangle \perp \ldots \perp \langle u_n, v_n \rangle$, where $(u_i, v_i) = 1$, $i = 1, \ldots, n$.*

Proof. We use induction on $\dim U$. It is clear that $\dim U \geq 2$. If $\dim U = 2$, there is nothing to prove. So assume that $\dim U > 2$

and that the result in the lemma is true for all non-degenerate submodules of U of dimension less than $\dim U$.

Let $\{w_1, \ldots, w_r\}$ be a basis of U, $r > 2$. We may assume that $(w_1, w_2) = 1$. For if $(w_1, w_i) \equiv 0 \pmod{q}$ for $i = 1, \ldots, r$, then $q^{\alpha-1}w_1 \in U^{\perp} = 0$, which is a contradiction; so (w_1, w_i) is invertible for some $2 \leq i \leq r$. Choose elements of U,

$$x_i = \xi_i w_1 + \eta_i w_2 + w_i, \quad i = 3, \ldots, r,$$

such that $x_i \in \langle w_1, w_2 \rangle^{\perp}$, $i = 3, \ldots, r$. This is done by taking $\xi_i = (w_2, w_i)$, $\eta_i = -(w_1, w_i)$. It is easily checked that $\{w_1, w_2, x_3, \ldots, x_r\}$ is linearly independent. Hence

$$U = \langle w_1, w_2 \rangle \perp V,$$

where $V = \langle x_3, \ldots, x_r \rangle$. Evidently $0 = U^{\perp} = V^{\perp}$ and $\dim V < \dim U$. Thus by the induction hypothesis, V is of the form in the lemma. Consequently U has the required form. //

If we remove the condition of "freeness" on our modules, we have

4.1.3 LEMMA. *Let U be a non-degenerate symplectic module over Z_{q^α}. Then $U = U_1 \perp \ldots \perp U_\alpha$, where $U_i = 0$ or*

$U_i = \langle u_{i1}, v_{i1} \rangle \perp \ldots \perp \langle u_{in_i}, v_{in_i} \rangle$, $1 \leq i \leq \alpha$, *and*

$(u_{ij}, v_{ij}) = q^{i-1}$, $j = 1, \ldots, n_i$, $1 \leq i \leq \alpha$.

Proof. We can consider U as a finite abelian q-group of exponent $\leq q^\alpha$ so that U is a direct sum of cyclic q-groups. If U is a homocyclic of exponent q^α, then U is a free non-degenerate symplectic module over Z_{q^α} and hence is taken care of by Lemma 4.1.2. However, if U is homocyclic of exponent q^β, $1 \leq \beta < \alpha$, we have

$$0 = (q^\beta x, y) = q^\beta (x, y) \quad \text{for all } x, y \in U,$$

ahd hence $(x, y) \equiv 0 \pmod{q^{\alpha-\beta}}$. In other words, $(x, y) = \lambda q^{\alpha-\beta}$

for some $0 \leq \lambda < q^{\beta}$. Clearly x, y determine λ uniquely modulo q^{β}. We can then turn U into a free non-degenerate symplectic module over $Z_{q^{\beta}}$ by defining the appropriate bilinear form on U as follows,

$$(\cdot, \cdot)_* : U \times U \to Z_{q^{\beta}},$$

$$(x, y)_* = q^{-(\alpha-\beta)}(x, y) \quad \text{for all} \quad x, y \in U.$$

It is a routine to check that $(\cdot, \cdot)_*$ has the desired properties. We can then apply Lemma 4.1.2 to U.

So assume that

$$U = \langle x_1 \rangle \oplus \ldots \oplus \langle x_s \rangle \oplus \langle y_1 \rangle \oplus \ldots \oplus \langle y_t \rangle,$$

where the order of x_i is q^{β}, $1 \leq \beta \leq \alpha$, for $i = 1, \ldots, s$, and $\langle y_1, \ldots, y_t \rangle$ is of exponent $< q^{\beta}$. Then $V = \langle x_1, \ldots, x_s \rangle$ is a free symplectic module over $Z_{q^{\beta}}$ by the preceding remarks. It is moreover non-degenerate. For suppose there exists $0 \neq x \in V \cap V^{\perp}$. If x is torsion-free, then $0 \neq q^{\beta-1}x \in V \cap V^{\perp}$. If x is a torsion element, then $x = q^{\delta}x'$ for some $1 \leq \delta < \beta$ and some torsion-free element x'. In any case, there is an element $0 \neq q^{\beta-1}x' \in V \cap V^{\perp}$. Hence

$$(q^{\beta-1}x', y) = (x', q^{\beta-1}y) = 0 \quad \text{for all} \quad y \in \langle y_1, \ldots, y_t \rangle,$$

and so $0 \neq q^{\beta-1}x' \in U^{\perp}$, which is a contradiction.

As remarked in the first paragraph, we have

$$V = \langle x'_1, x'_2 \rangle \perp \ldots \perp \langle x'_{2m-1}, x'_{2m} \rangle,$$

where $(x'_{2i-1}, x'_{2i}) = q^{\alpha-\beta}$, $i = 1, \ldots, m$. We now use induction on α to complete the proof. If $\alpha = 1$, there is nothing to prove. So assume that $\alpha > 1$ and that the result in the lemma holds for all non-degenerate symplectic modules over $Z_{q^{\gamma}}$ where $1 \leq \gamma < \alpha$. First

we choose elements of U ,

$$w_i = \sum_{j=1}^{2m} \xi_{ij} x'_j + y_i \ , \quad i = 1, \ldots, t \ ,$$

such that $w_i \in V^{\perp}$, $i = 1, \ldots, t$. This is done by taking

$$\xi_{i,2j-1} = (x'_{2j}, y_i) \ , \quad \xi_{i,2j} = -(x'_{2j-1}, y_i) \ , \quad j = 1, \ldots, m \ .$$

Evidently $U = V \perp W$ where $W = \langle w_1, \ldots, w_t \rangle$. Since U is non-degenerate, W must also be non-degenerate (over Z_{q^α}).

We claim that W is of exponent $\leq q^{\beta-1}$. For we have $q^{\beta-1}\xi_{i,2j-1} = \left(x'_{2j}, q^{\beta-1}y_i\right) = 0$ and similarly, $q^{\beta-1}\xi_{i,2j} = 0$. Hence $q^{\beta-1}w_i = 0$, $i = 1, \ldots, t$. Moreover, $(w, w') \equiv 0 \pmod{q^{\alpha-\beta+1}}$ for all $w, w' \in W$ since $q^{\beta-1}(w, w') = (q^{\beta-1}w, w') = 0$. We can then turn W into a non-degenerate symplectic module over $Z_{q^{\beta-1}}$ by defining an appropriate bilinear form on W as follows,

$$(\cdot, \cdot)_* : W \times W \to Z_{q^{\beta-1}} \ ,$$

$$(w, w')_* = q^{-(\alpha-\beta+1)}(w, w') \quad \text{for all } w, w' \in W \ .$$

That $(\cdot, \cdot)_*$ satisfies the required conditions is easily verified. Since $\beta-1 < \alpha$, we can apply the induction hypothesis to W to get

$$W = W_1 \perp \ldots \perp W_{\beta-1} \ ,$$

where $W_i = 0$ or $W_i = \langle x_{i1}, y_{i1} \rangle \perp \ldots \perp \left\langle x_{im_i}, y_{im_i} \right\rangle$,

$i = 1, \ldots, \beta-1$, and $(x_{ij}, y_{ij})_* = q^{i-1}$, $j = 1, \ldots, m_i$,

$1 \leq i \leq \beta-1$. Write $u_{\alpha-\beta+1,i} = x'_{2i-1}$, $v_{\alpha-\beta+1,i} = x'_{2i}$,

$i = 1, \ldots, m$,

$u_{\alpha-\beta+i+1,j} = x_{ij}$, $v_{\alpha-\beta+i+1,j} = y_{ij}$, $j = 1, \ldots, m_i$, $1 \leq i \leq \beta-1$,

$$U_{\alpha-\beta+1} = V \ , \quad U_{\alpha-\beta+i+1} = W_i \ , \quad i = 1, \ldots, \beta-1 \ .$$

Then U has the required form in the lemma. //

A decomposition of U of the above form is called a *symplectic*

decomposition of U, and the set of ordered pairs of elements of U, $\{[u_{ij}, v_{ij}] : j = 1, \ldots, n_i, \ 1 \leq i \leq \alpha\}$, is called a *symplectic set* corresponding to that particular decomposition of U. Thus we can associate to each non-degenerate symplectic module U over Z_{q^α} a finite sequence $[n_1, \ldots, n_\alpha]$ where we set $n_i = 0$ if $U_i = 0$ in the above decomposition of U. We call $[n_1, \ldots, n_\alpha]$ the *symplectic sequence* of U. The following theorem will justify our calling it so. But first we define isomorphism between two non-degenerate symplectic modules U and V over Z_{q^α}. U and V are said to be *isomorphic* if there is a module isomorphism $\tau : U \to V$ from U onto V such that $(u\tau, u'\tau)_0 = (u, u')$ for all $u, u' \in U$, where $(\cdot, \cdot)$ and $(\cdot, \cdot)_0$ are the bilinear forms on U and V respectively.

4.1.4 THEOREM. *Two non-degenerate symplectic modules over* Z_{q^α} *are isomorphic if and only if they have the same symplectic sequence.*

Proof. Let symplectic decompositions of the non-degenerate symplectic modules U and V over Z_{q^α} be given by

$$U = U_1 \perp \ldots \perp U_\alpha ,$$

where $U_i = \langle u_{i1}, v_{u1} \rangle \perp \ldots \perp \langle u_{in_i}, v_{in_i} \rangle$, $i = 1, \ldots, \alpha$, and $V = V_1 \perp \ldots \perp V_\alpha$, where $V_i = \langle x_{i1}, y_{i1} \rangle \perp \ldots \perp \langle x_{im_i}, y_{im_i} \rangle$, $i = 1, \ldots, \alpha$.

Suppose that U and V are isomorphic. Then there is a module isomorphism τ from U onto V such that

$$(u\tau, u'\tau) = (u, u') \text{ for all } u, u' \in U ,$$

where we have also denoted the bilinear form on V by $(\cdot, \cdot)$ since there is no confusion in doing so. Write

$$x'_{ij} = u_{ij}\tau , \quad y'_{ij} = v_{ij}\tau , \quad j = 1, \ldots, n_i , \quad 1 \leq i \leq \alpha ,$$

and $V'_i = U_i\tau$, $i = 1, \ldots, \alpha$. Then $V = U\tau = V'_1 \perp \ldots \perp V'_\alpha$, where

$V_i' = \langle x_{i1}', y_{i1}' \rangle \perp \ldots \perp \langle x_{in_i}', y_{in_i}' \rangle$, $i = 1, \ldots, \alpha$. We claim that x_{ij}' and y_{ij}' each has order $q^{\alpha-i+1}$. For we have

$$\left(q^{\alpha-i+1}x_{ij}', y_{ij}'\right) = q^{\alpha-i+1}(x_{ij}', y_{ij}') = 0 ,$$

and so $q^{\alpha-i+1}x' = 0$, but $q^{\alpha-i}x' \neq 0$ since $\left(q^{\alpha-i}x_{ij}', y_{ij}'\right) = q^{\alpha-1} \neq 0$. Thus considered as a finite abelian q-group, V is a direct sum of $2n_1$ q^{α}-cycles , $2n_2$ $q^{\alpha-1}$-cycles , ... , and $2n_\alpha$ q-cycles. Likewise the decomposition $V = V_1 \perp \ldots \perp V_\alpha$ shows that V is a direct sum of $2m_1$ q^{α}-cycles, $2m_2$ $q^{\alpha-1}$-cycles , ... , and $2m_\alpha$ q-cycles. Hence by the isomorphism theorem for abelian groups, we must have $n_i = m_i$, $i = 1, \ldots, \alpha$; or U and V have the same symplectic sequence.

Conversely suppose that U and V have the same symplectic sequence, that is, $n_i = m_i$, $i = 1, \ldots, \alpha$. If we define the mapping $\tau : U \to V$ by

$$u_{ij}\tau = x_{ij} , \quad v_{ij}\tau = y_{ij} , \quad j = 1, \ldots, n_i , \quad 1 \leq i \leq \alpha ,$$

then it is clear that τ can be extended by linearity to a module isomorphism from U onto V such that

$$(u\tau, u'\tau) = (u, u') \quad \text{for all } u, u' \in U .$$

Hence U and V are isomorphic. //

We say that U is a *canonic non-degenerate symplectic module* over Z_{q^α} if its symplectic sequence is $[n_1, \ldots, n_\alpha]$ with $n_1 > 0$. Thus if U is canonic, there are elements $u, v \in U$ such that $(u, v) = 1$. What is of interest is that it is always possible to reduce any non-degenerate symplectic module to a canonic one as the next lemma shows.

4.1.5 LEMMA. *Every non-degenerate symplectic module over* Z_{q^α} *uniquely determines up to isomorphism a canonic non-degenerate symplectic module over* Z_{q^β} *for some* $1 \leq \beta \leq \alpha$.

Proof. With the usual notations, we choose some symplectic decomposition of the non-degenerate symplectic module U over Z_{q^α},

$$U = U_1 \perp \dots \perp U_\alpha ,$$

and let the symplectic sequence of U be $[n_1, \dots, n_\alpha]$. If $n_1 > 0$, there is nothing to prove. So let γ be the smallest integer $1 < \gamma \leq \alpha$ for which $n_\gamma > 0$. Then

$$U = U_\gamma \perp \dots \perp U_\alpha .$$

Write $\beta = \alpha - \gamma + 1$. We claim that U has exponent q^β. Since $(u_{ij}, v_{ij}) = q^{i-1}$, we have for each $\gamma \leq i \leq \alpha$,

$$\left(q^\beta u_{ij}, v_{ij}\right) = q^{\beta+i-1} = 0 .$$

Hence $q^\beta u_{ij} \in U^\perp$ and so $q^\beta u_{ij} = 0$. Similarly $q^\beta v_{ij} = 0$. This holds for all $i = \gamma, \gamma+1, \dots, \alpha$. Moreover $q^{\beta-1} u_{\gamma 1} \neq 0$ since $\left(q^{\beta-1} u_{\gamma 1}, v_{\gamma 1}\right) = q^{\alpha-1} \neq 0$, and so U has exponent q^β.

We can then consider U as a Z_{q^β}-module U^*. Evidently $(u, v) \equiv 0 \pmod{q^{\alpha-\beta}}$ for all $u, v \in U$. Thus we can define as before a suitable Z_{q^β}-bilinear form on U^* by

$$(\cdot, \cdot)_* : U^* \times U^* \to Z_q ,$$

$$(u, v)_* = q^{-(\gamma-1)}(u, v) \quad \text{for all } u, v \in U^* .$$

Clearly $(\cdot, \cdot)_*$ is non-degenerate. Writing

$$U_i^* = U_{\gamma+i-1} , \quad i = 1, \dots, \beta ,$$

we have $U^* = U_1^* \perp \dots \perp U_\beta^*$, where $U_1^* \neq 0$, and the symplectic sequence of U^* is $[n_\gamma, n_{\gamma+1}, \dots, n_\alpha]$ with $n_\gamma > 0$. Hence U^* is a canonic non-degenerate symplectic module over Z_{q^β} and is uniquely determined up to isomorphism, by virtue of Theorem 4.1.4. //

Thus we can speak of the canonic non-degenerate symplectic module U^* (over Z_{q^β}) corresponding to each non-degenerate sumplectic module U over Z_{q^α}. It turns out that U is, in fact, determined by U^*.

4.1.6 THEOREM. *Two non-degenerate symplectic modules (over Z_{q^α}) are isomorphic if and only if their corresponding canonic non-degenerate symplectic modules are isomorphic.*

Proof. Let U and V be two non-degenerate symplectic modules over Z_{q^α}, and let their corresponding canonic modules be U^* (over Z_{q^β}) and V^* (over $Z_{q^{\beta'}}$) respectively. Suppose the symplectic sequences of U and V are $[n_1, \ldots, n_\alpha]$ and $[n'_1, \ldots, n'_\alpha]$ respectively. Then by the construction in the proof of Lemma 4.1.5, the symplectic sequence of U^* is $[n_\gamma, \ldots, n_\alpha]$ where $\beta = \alpha - \gamma + 1$ and γ is the smallest integer $1 \le \gamma \le \alpha$ for which $n_\gamma > 0$. Likewise the symplectic sequence of V^* is $[n'_{\gamma'}, \ldots, n'_\alpha]$ where $\beta' = \alpha - \gamma' + 1$ and γ' is the smallest integer $1 \le \gamma' \le \alpha$ for which $n_{\gamma'} > 0$. By Theorem 4.1.4, U and V are isomorphic if and only if $[n_1, \ldots, n_\alpha] = [n'_1, \ldots, n'_\alpha]$, that is, if and only if $[n_\gamma, \ldots, n_\alpha] = [n'_{\gamma'}, \ldots, n'_\alpha]$, that is, if and only if U^* and V^* are isomorphic. //

An automorphism φ of a non-degenerate symplectic module U (over Z_{q^α}) is called an *isometry* of U if φ preserves the bilinear form on U, that is, $(u\varphi, v\varphi) = (u, v)$ for all $u, v \in U$. It is clear that the isometries of U form a group which we denote by $Sp(U)$. The next two lemmas show that we need only study $Sp(U)$ for a canonic non-degenerate symplectic module U over Z_{q^α}. Since U is determined by its symplectic sequence $[n_1, \ldots, n_\alpha]$, there is no ambiguity in writing $Sp(n_\alpha, \ldots, n_1)$ for $Sp(U)$ whether U is canonic or not. It is for a later convenience that we use this alternative notation.

4.1.7 LEMMA. *Let U be a non-degenerate symplectic module over Z_{q^α} and U^* its canonic symplectic module. Then $Sp(U) \cong Sp(U^*)$.*

Proof. Let $\varphi \in Sp(U)$. Clearly φ induces naturally an automorphism φ^* of U^* . Moreover φ^* preserves the bilinear form $(\cdot, \cdot)_*$ on U^* since

$$(u\varphi^*, v\varphi^*)_* = q^{-(\gamma-1)}(u\varphi, v\varphi) = q^{-(\gamma-1)}(u, v) = (u, v)_*$$

for all $u, v \in U^*$, where we have used the notations in the proof of Lemma 4.1.5. Hence $\varphi^* \in Sp(U^*)$. Conversely, $\varphi^* \in Sp(U^*)$ induces in the obvious way an automorphism φ of U . As before, it is easily checked that $\varphi \in Sp(U)$. The mapping $\varphi \mapsto \varphi^*$ gives the required isomorphism of $Sp(U)$ onto $Sp(U^*)$. //

4.1.8 LEMMA. *If U and V are two isomorphic non-degenerate symplectic modules (over Z_{q^α}) , then $Sp(U) \cong Sp(V)$.*

Proof. In view of the preceding lemma, we may assume that U and V are canonic. Fix some symplectic decomposition of U ,

$$U = U_1 \perp \dots \perp U_\alpha ,$$

where $U_i = \langle x_{i1}, y_{i1} \rangle \perp \dots \perp \langle x_{in_i}, y_{in_i} \rangle$, $i = 1, \dots, \alpha$.

Let $\tau : U \to V$ be the isomorphism of U onto V . Write

$$x'_{ij} = x_{ij}\tau , \quad y'_{ij} = y_{ij}\tau , \quad j = 1, \dots, n_i , \quad 1 \le i \le \alpha ,$$

and $V_i = \langle x'_{i1}, y'_{i1} \rangle \perp \dots \perp \langle x'_{in_i}, y'_{in_i} \rangle$, $i = 1, \dots, \alpha$. Then $V = V_1 \perp \dots \perp V_\alpha$ is a symplectic decomposition of V . Let $\varphi \in Sp(U)$ where

$$x_{ij}\varphi = u_{ij} , \quad y_{ij}\varphi = v_{ij} , \quad j = 1, \dots, n_i , \quad 1 \le i \le \alpha .$$

Define $\varphi' : V \to V$ by

$$x'_{ij}\varphi' = u_{ij}\tau , \quad y'_{ij}\varphi' = v_{ij}\tau , \quad j = 1, \dots, n_i , \quad 1 \le i \le \alpha .$$

Clearly $\varphi' \in Sp(V)$. Moreover it is easily checked that $\tau\varphi' = \varphi\tau$.

Consider the mapping $\varphi \mapsto \varphi'$. It is plainly one-to-one and onto. We verify that it is a homomorphism. Let $\varphi \mapsto \varphi'$,

$\varphi^{-1} \mapsto (\varphi^{-1})'$. Then

$$\tau(\varphi^{-1})' = \varphi^{-1}\tau = \tau\varphi'^{-1} ,$$

and so $(\varphi^{-1})' = \varphi'^{-1}$. Finally let $\varphi_i \mapsto \varphi_i'$, $i = 1, 2$, and $\varphi_1\varphi_2 \mapsto (\varphi_1\varphi_2)'$. Then

$$\tau(\varphi_1\varphi_2)' = \varphi_1\varphi_2\tau = \varphi_1\tau\varphi_2' = \tau\varphi_1'\varphi_2' ,$$

and hence $(\varphi_1\varphi_2)' = \varphi_1'\varphi_2'$. //

Note that if the symplectic sequence of U is $[0, \ldots, 0, n_\gamma, \ldots, n_\alpha]$ where $n_\gamma > 0$, $1 < \gamma \leq \alpha$, then Lemma 4.1.7 is equivalent to saying that $Sp(n_\alpha, \ldots, n_\gamma, 0, \ldots, 0) \cong Sp(n_\alpha, \ldots, n_\gamma)$ where $[n_\gamma, \ldots, n_\alpha]$ is the symplectic sequence of U^* .

A set of ordered pairs of elements of U , $\{[u_{ij}, v_{ij}] : j = 1, \ldots, n_i, 1 \leq i \leq \alpha\}$, is called a *symplectic set* for U if it is a symplectic set corresponding to some symplectic decomposition of U (see the remarks immediately preceding Theorem 4.1.4). Lemma 4.1.3 tells us that every non-degenerate symplectic module has a symplectic set. The following property of symplectic sets will be useful.

4.1.9 LEMMA. *Let V and W be non-degenerate symplectic modules over Z_{q^α} , and let S and T be symplectic sets for V and W respectively. Then $S \cup T$ is a symplectic set for $U = V \perp W$.*

Proof. Let the sumplectic sequences of V and W be $[m_1, \ldots, m_\alpha]$ and $[n_1, \ldots, n_\alpha]$ respectively. Suppose that

$$S = \{[a_{ij}, b_{ij}] : j = 1, \ldots, m_i , 1 \leq i \leq \alpha\} ,$$

$$T = \{[c_{ij}, d_{ij}] : j = 1, \ldots, n_i , 1 \leq i \leq \alpha\} .$$

Then

$$V = V_1 \perp \ldots \perp V_\alpha ,$$

$$W = W_1 \perp \ldots \perp W_\alpha ,$$

where

$$V_i = \langle a_{i1}, b_{i1} \rangle \perp \ldots \perp \langle a_{in_i}, b_{in_i} \rangle ,$$

$$W_i = \langle c_{i1}, d_{i1} \rangle \perp \ldots \perp \langle c_{in_i}, d_{in_i} \rangle ,$$

for $i = 1, \ldots, \alpha$, are symplectic decompositions of V and W. It is then clear that $U = U_1 \perp \ldots \perp U_\alpha$, where $U_i = V_i \perp W_i$, $i = 1, \ldots, \alpha$, is a symplectic decomposition of $U = V \perp W$, and hence $S \cup T$ is the corresponding symplectic set. //

We introduce the notion of a hyperbolic pair of a canonic non-degenerate symplectic module U over Z_q^α. An ordered pair $[u, v]$ of elements of U is called a *hyperbolic pair* of U if $(u, v) = 1$. We denote the set of hyperbolic pairs of U by $\Omega(U)$ and write $\omega(U) = |\Omega(U)|$. Alternatively we write $\omega(n_\alpha, \ldots, n_1) = \omega(U)$ where $[n_1, \ldots, n_\alpha]$ is the symplectic sequence of U.

We do not know if there is an analogue of Witt's Theorem (9.9, Chapter II, Huppert [16]) for symplectic modules. The following weaker versions will suffice for our purposes.

4.1.10 LEMMA. *Let $[u, v]$ be a hyperbolic pair of a free non-degenerate symplectic module U over Z_q^α. Then $\{[u, v]\}$ can be extended to a symplectic set for U.*

Proof. If $\dim U = 2$, there is nothing to prove. So suppose $\dim U > 2$. Evidently $\{u, v\}$ is linearly independent and so by Lemma 4.1.1, can be extended to a basis of U, $\{u, v, w_3, \ldots, w_r\}$ say. As in the proof of Lemma 4.1.2, we can construct a non-degenerate submodule V such that

$$U = \langle u, v \rangle \perp V .$$

By Lemma 4.1.2, there is a symplectic set S for V. Hence by Lemma 4.1.9, $\{[u, v]\} \cup S$ is a symplectic set for U. //

4.1.11 LEMMA. *Let $[u, v]$ be a hyperbolic pair of a canonic non-degenerate symplectic module U over Z_q^α. Then $\{[u, v]\}$ can*

be extended to a symplectic set for U .

Proof. With the notations of Lemma 4.1.3, we fix a symplectic decomposition

$$U = U_1 \perp \dots \perp U_\alpha .$$

First we prove the lemma with $n_1 = 1$, so that $U_1 = \langle u_{11}, v_{11} \rangle$. If $\alpha = 1$, there is nothing to prove. So suppose $\alpha > 1$, and write $V = U_2 \perp \dots \perp U$. Let

$$u = a + c , \quad v = b + d , \quad a, b \in U_1 , \quad c, d \in V .$$

Since $(c, d) \equiv 0 \pmod{q}$, (a, b) is invertible. Hence $U_1 = \langle a, b \rangle$ and $U = \langle u, v \rangle \oplus V$. For each $2 \le i \le \alpha$, we can choose elements of U ,

$$x_{ij} = \lambda_{ij} u + \mu_{ij} v + u_{ij} , \quad y_{ij} = \rho_{ij} u + \sigma_{ij} v + v_{ij}$$

for $j = 1, \dots, n_i$, such that $x_{ij}, y_{ij} \in \langle x, y \rangle^{\perp}$. Clearly then

$$U = \langle u, v \rangle \perp W ,$$

where $W = \langle x_{ij}, y_{ij} : j = 1, \dots, n_i , \ 2 \le i \le \alpha \rangle$ is plainly non-degenerate, and hence has a symplectic set S by Lemma 4.1.3. It then follows from Lemma 4.1.9 that $\{[u, v]\} \cup S$ is a symplectic set for U .

Suppose now $n_1 > 1$. With the above notations, we may assume that $(a, b) = 1$. If we apply the preceding lemma to U_1 , we obtain a symplectic set $\left\{[a, b], [a_2, b_2], \dots, \left[a_{n_1}, b_{n_1}\right]\right\}$ for U_1 , so that $U_1 = \langle a, b \rangle \perp \langle a_2, b_2 \rangle \perp \dots \perp \left\langle a_{n_1}, b_{n_1} \right\rangle$. Put $V' = \langle a, b \rangle \perp V$. Then $[u, v]$ is a hyperbolic pair of V' and so by what has been proved for the case $n_1 = 1$, $\{[u, v]\}$ can be extended to a symplectic set $\{[u, v]\} \cup T_1$ for V' . But

$$U = V' \perp W' ,$$

where $W' = \langle a_2, b_2 \rangle \perp \dots \perp \left\langle a_{n_1}, b_{n_1} \right\rangle$, and

$T_2 = \{[a_i, b_i] : i = 2, \ldots, n_1\}$ is a symplectic set for W'. So by Lemma 4.1.9, $\{[u, v]\} \cup T_1 \cup T_2$ is a symplectic set for U. //

The next lemma shows that $Sp(U)$ behaves very much like the symplectic group; see, for example, Huppert [16].

4.1.12 LEMMA. *Let U be a canonic non-degenerate symplectic module over Z_{q^α}. Then $Sp(U)$ acts transitively on $\Omega(U)$.*

Proof. For every $[u, v] \in \Omega(U)$ and $\varphi \in Sp(U)$, $[u\varphi, v\varphi] \in \Omega(U)$ since $(u\varphi, v\varphi) = (u, v) = 1$.

Let $[u, v], [u', v'] \in \Omega(U)$. By the preceding lemma, $\{[u, v]\}$ and $\{[u', v']\}$ can be extended to symplectic sets for U. In other words, there are symplectic decompositions

$$U = U_1 \perp \ldots \perp U_\alpha, \quad U = U_1' \perp \ldots \perp U_\alpha',$$

where

$$U_i = \langle u_{i1}, v_{i1} \rangle \perp \ldots \perp \langle u_{in_i}, v_{in_i} \rangle,$$

$$U_i' = \langle u_{i1}', v_{i1}' \rangle \perp \ldots \perp \langle u_{in_i}', v_{in_i}' \rangle,$$

and $(u_{ij}, v_{ij}) = q^{i-1} = (u_{ij}', v_{ij}')$, $j = 1, \ldots, n_i$, $1 \le i \le \alpha$, and $u = u_{11}$, $v = v_{11}$, $u' = u_{11}'$, $v' = v_{11}'$. It is then clear that the mapping $\varphi : U \to U$ given by

$$u_{ij}\varphi = u_{ij}', \quad v_{ij}\varphi = v_{ij}', \quad j = 1, \ldots, n_i, \quad 1 \le i \le \alpha.$$

determines an element of $Sp(U)$. Also $[u, v] = [u', v']$. Thus if we define the action of $Sp(U)$ on $\Omega(U)$ by $\varphi : [u, v] \mapsto [u\varphi, v\varphi]$, this action is transitive. //

We now begin the enumeration process for the calculation of $|Sp(n_\alpha, \ldots, n_1)|$ with $n_1 > 0$.

4.1.13 LEMMA. *Let U be a canonic non-degenerate symplectic module over Z_{q^α} with symplectic sequence $[n_1, \ldots, n_\alpha]$, and let $[u, v] \in \Omega(U)$. Then $\{\varphi \in Sp(U) : u\varphi = u, v\varphi = v\} \cong Sp(n_\alpha, \ldots, n_2, n_1 - 1)$.*

Proof. By Lemma 4.1.11, there is a symplectic decomposition

$$U = U_1 \perp \dots \perp U_\alpha ,$$

where $U_i = \langle u_{i1}, v_{i1} \rangle \perp \dots \perp \langle u_{in_i}, v_{in_i} \rangle$, $i = 1, \dots, \alpha$, and $u = u_{11}$, $v = v_{11}$. Let $\varphi \in Sp(U)$ such that $u\varphi = u$, $v\varphi = v$. Then for $1 < j \leq n_1$, $(u, u_{1j}\varphi) = (u\varphi, u_{1j}\varphi) = (u, u_{1j}) = 0$. Likewise we can easily show that $u_{ij}\varphi, v_{ij}\varphi \in \langle u, v \rangle^{\perp}$ for $j = 2, \dots, n_1$ if $i = 1$, and for $j = 1, \dots, n_i$ if $1 < i \leq \alpha$. In other words, if we put

$$V = \langle u_{12}, v_{12} \rangle \perp \dots \perp \langle u_{1n_1}, v_{1n_1} \rangle \perp U_2 \perp \dots \perp U_\alpha ,$$

then $\varphi|_V \in Sp(U)$. Conversely given any element of $Sp(U)$ we can obviously extend it to an element $\varphi \in Sp(U)$ such that $u\varphi = u$, $v\varphi = v$. Moreover the symplectic sequence of V is $[n_1-1, n_2, \dots, n_\alpha]$ and hence the above mapping gives the required isomorphism. //

This enables us to reduce the calculation to an enumeration of the hyperbolic pairs of U .

4.1.14 LEMMA. $|Sp(n_\alpha, \dots, n_1)| = \prod_{i=1}^{\alpha} \prod_{j=1}^{n_i} \omega(n_\alpha, \dots, n_{i+1}, j)$, $n_1 > 0$.

Proof. By Lemmas 4.1.12 and 4.1.13 and a well-known theorem on permutation groups (5.11, Chapter I, Huppert [16]),

$$|Sp(n_\alpha, \dots, n_1)| = \omega(n_\alpha, \dots, n_1) \cdot |Sp(n_\alpha, \dots, n_2, n_1-1)| .$$

Recall that $Sp(n_\alpha, \dots, n_i, 0) \cong Sp(n_\alpha, \dots, n_i)$ in view of Lemma 4.1.7. A repeated application of the recurrence relation gives the desired expression. //

We call an ordered pair $[u, v]$ of elements of U an *invertible pair* of U if (u, v) is invertible.

4.1.15 LEMMA. *Let V be a free non-degenerate symplectic module of dimension n over Z_{q^β} . Then*

$$\omega(V) = q^{(2n-1)\beta+2n(\beta-1)}(q^{2n}-1) .$$

Proof. We calculate the number of invertible pairs of V in two different ways. First suppose x is a torsion-free element of V. Then there is an element $x' \in V$ such that $(x, x') = 1$. By Lemma 4.1.10,

$$V = \langle x, x' \rangle \perp W ,$$

where $\dim W = 2(n-1)$. Let $y = \xi x + \xi' x' + w$, where $\xi, \xi' \in Z_{q^\beta}$, $w \in W$. Then $(x, y) = \xi'$, and so (x, y) is invertible if and only if ξ' is. Thus for a fixed torsion-free element x, there are $q^{(2n-1)\beta}(q^\beta - q^{\beta-1})$ elements y such that (x, y) is invertible. But there are $(q^{2n\beta} - q^{2n(\beta-1)})$ distinct torsion-free elements in V. Hence the total number of invertible paris of V is $q^{(2n-1)\beta}(q^\beta - q^{\beta-1})(q^{2n\beta} - q^{2n(\beta-1)})$.

Next consider for every hyperbolic pair $[u, v]$ the following set of invertible pairs

$$S[u, v] = \{[u, \lambda v] : \lambda \text{ is invertible in } Z_{q^\beta}\} .$$

We claim that $[u, v] \neq [u', v']$ implies that $S[u, v] \cap S[u', v']$ is empty. If not, then $[u, \lambda v] = [u', \lambda' v']$ for some invertible $\lambda, \lambda' \in Z_{q^\beta}$. Hence $u = u'$, $\lambda v = \lambda' v'$ and so $\lambda(u, v) = \lambda'(u', v')$, or $\lambda = \lambda'$. Moreover $S[u, v]$ consists of exactly $(q^\beta - q^{\beta-1})$ distinct invertible pairs as the number of invertible elements of Z_{q^β} is $q^\beta - q^{\beta-1}$. Furtheremore every invertible pair $[x, y]$ belongs to $S[u, v]$ where $u = x$, $v = (x, y)^{-1} y$. Therefore the total number of invertible pairs of V is $\omega(V).(q^\beta - q^{\beta-1})$. Equating the two expressions for the same quantity, we get the required result. //

4.1.16 LEMMA. *Let* $n_1 > 0$. *Then*

$$\log_q \omega(n_\alpha, \ldots, n_1) = (2n_1 - 1)\alpha + 2n_1(\alpha-1) + 4 \sum_{i=2}^{\alpha} n_i(\alpha - i + 1) + \log_q (q^{2n_1} - 1) .$$

Proof. With the notations of Lemma 4.1.3, fix a symplectic

decomposition

$$U = U_1 \perp \dots \perp U_\alpha .$$

Write $V = U_2 \perp \dots \perp U_\alpha$. Let $x, y \in U$ and suppose

$$x = a + c , \quad y = b + d , \quad a, b \in U_1 , \quad c, d \in V .$$

Then $(x, y) = (a, b) + (c, d)$. Since $(c, d) \equiv 0 \pmod q$ for all $c, d \in V$, it follows that (x, y) is invertible if and only if (a, b) is. If we denote the number of distinct elements of V by $|V|$, the total number of invertible pairs of U is then equal to

$$|V|^2 \times \text{the number of invertible pairs of } U_1 .$$

As in the proof of the preceding lemma, we have that the number of invertible pairs of U_1 is $\omega(U_1).(q^\alpha - q^{\alpha-1})$ and that the number of invertible pairs of U is also equal to $\omega(U).(q^\alpha - q^{\alpha-1})$. Hence

$$\omega(U) = \omega(U_1).|V|^2 ,$$

and $\omega(U_1)$ is given by Lemma 4.1.15. We also know from the proof of Theorem 4.1.4 that V as an abelian group is a direct sum of $2n_2$ $q^{\alpha-1}$-cycles, $2n_3$ $q^{\alpha-2}$-cycles, ... , and $2n_\alpha$ q-cycles, so that $\log_q|V| = 2 \sum_{i=2}^{\alpha} n_i(\alpha-i+1)$. Hence we have the desired expression for $\omega(U)$. //

It will be convenient to use the logarithmic notation.

4.1.17 THEOREM. *Let* $n_1 > 0$. *Then*

$$\log_q|Sp(n_\alpha, \dots, n_1)| = \sum_{i=1}^{\alpha} \left\{(2\alpha-2i+1)n_i^2+(\alpha-i)n_i\right\} + 4 \sum_{i=1}^{\alpha-1} \sum_{j=i}^{\alpha-1} (\alpha-j)n_i n_{j+1} + \sum_{i=1}^{\alpha} \sum_{j=1}^{n_i} \log_q(q^{2j}-1) .$$

Proof. Write $m_1 = j$, $m_2 = n_{i+1}$, ..., $m_\beta = n_\alpha$, where $\beta = \alpha - i + 1$. Then by Lemma 4.1.16,

$$\log_q \omega(m_\beta, \ldots, m_1)$$

$$= (2j-1)(\alpha-i+1) + 2j(\alpha-i) + 4 \sum_{k=i+1}^{\alpha} n_k(\alpha-k+1) + \log_q(q^{2j}-1) .$$

From the formula of Lemma 4.1.14, we obtain the required expression. //

4.2 Linear automorphisms of irreducible linear groups in $\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_{q^n}$, q odd

We denote the group of automorphisms of a group G by aut G, and the group of inner automorphisms of G by inn G. In addition, we write $\text{aut}_Z G = \{\varphi \in \text{aut } G : z\varphi = z \text{ for all } z \in Z(G)\}$. In this section G will be an irreducible linear group over some splitting field E, and G belongs as abstract group to $\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_{q^n}$, q odd. Thus $G \leq \text{GL}(r, E)$. The group of *linear automorphisms* of G, denoted by lin aut G, is defined as

$$\text{lin aut } G = \{\varphi \in \text{aut } G : \text{there exists } y \in \text{GL}(r, E) \text{ such that } x\varphi = y^{-1}xy \text{ for all } x \in G\} .$$

We will use the notations and terminologies of Chapter 2 and 4.1 without further ado.

The aim of this section is to calculate the order of lin aut G. We describe the gist of the method first and prove the main results with reference to the details which will be given from Lemma 4.2.10 onwards. We begin the reduction process with

4.2.1 LEMMA. *Let G be an irreducible linear group in $\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_{q^n}$. Then* $\text{aut}_Z G = \text{lin aut } G$.

Proof (L.G. Kovács). By 4.1.6, Brady [3], every automorphism of $Z(G)$ is the restriction to $Z(G)$ of an automorphism of G. Hence we have the epimorphism $R : \text{aut } G \twoheadrightarrow \text{aut } Z(G)$. If $Z(G)$ is cyclic of order q^l, then $|\text{aut } Z(G)| = q^{l-1}(q-1)$. Moreover by 2.9, Brady, Bryce and Cossey [4], there are $q^{l-1}(q-1)$ inequivalent faithful irreducible representations of G over a splitting field. Thus the number of inequivalent faithful irreducibles of G is equal to $|\text{aut } Z(G)|$.

We claim that aut G acts transitively on the equivalence classes of the faithful irreducibles of G. Let $\rho : G \to GL(r, E)$ be a faithful irreducible representation of G. Then it is clear that for every $\alpha \in$ aut G, $\alpha\rho$ is also a faithful irreducible of G. Now let ρ and σ be faithful irreducibles of G. Then since G has only one linear isomorphism class of faithful irreducibles by 2.4, Brady, Bryce and Cossey [4],

$$G\rho = (G\sigma)^u \quad \text{for some} \quad u \in GL(r, E) .$$

Define $\alpha : G \to G$ by $g\alpha = h$ where $g\rho = (h\sigma)^u$. Clearly $\alpha \in$ aut G and $\rho \sim \alpha\sigma$ where $\sim$ denotes equivalence of representations. If we define the action of aut G on the equivalence classes of faithful irreducibles of G by $\alpha : [\rho] \mapsto [\alpha\rho]$, where $\alpha \in$ aut G and $[\rho]$ is the equivalence class to which ρ belongs, then the action is transitive.

By a result on permutation groups,

$|\text{aut } G|/|A_0|$

= number of inequivalent faithful irreducibles of $G = |\text{aut } Z(G)|$,

where $A_0 = \{\alpha \in \text{aut } G : \alpha\rho \sim \rho\}$ for a fixed faithful irreducible ρ. Since aut $G/\ker R \cong$ aut $Z(G)$, it follows that $|\ker R| = |A_0|$. But $A_0 \leq \ker R$; for by Lemma 2.1, Chapter 3, Gorenstein [9], $z\rho$ is scalar for all z in $Z(G)$, and hence $g\alpha\rho = u^{-1}(g\rho)u$ implies that for all $z \in Z(G)$, $z\alpha\rho = u^{-1}(z\rho)u = z\rho$, that is, $z\alpha = z$. Therefore $A_0 = \ker R$.

Finally if we consider G as a subgroup of $GL(r, E)$ and take ρ to be the identity mapping, then A_0 consists of precisely the linear automorphisms of G, that is, $A_0 = \text{lin aut } G$. Evidently $\ker R = \text{aut}_Z G$, and hence $\text{aut}_Z G = \text{lin aut } G$. //

In view of the above lemma, we need only consider G as an abstract group. In the rest of this section, unless stated otherwise, G will be assumed to have the given canonic decomposition

$$G \cong Q(n_1, r_1) \ldots Q(n_\alpha, r_\alpha)Q(l)^{\varepsilon_l} \ldots Q(1)^{\varepsilon_1} ,$$

where $\alpha \geq 1$, $r_\alpha > 0$, $\varepsilon_l > 0$, and $Q(i, i)$ has been abbreviated to $Q(i)$. Choose canonic generators a_i, b_i, a_{jk}, b_{jk}, $i = 1, \ldots, \alpha$, $k = 1, \ldots, \varepsilon_j$, $1 \leq j \leq l$, to satisfy Lemma 4.2.9. These will be kept fixed throughout the discussion on G. Consider the abelian factor group

$$U = G/Z(G)$$
$$= \langle \bar{a}_i, \bar{b}_i, \bar{a}_{jk}, \bar{b}_{jk} : i = 1, \ldots, \alpha, \ k = 1, \ldots, \varepsilon_j, \ 1 \leq j \leq l \rangle .$$

For every $x \in G$, we write $\bar{x}$ for the corresponding coset $xZ(G)$ in U. By Lemma 4.2.9, $Z(G)$ is the largest of the following subgroups, $\langle [a_{l1}, b_{l1}] \rangle$, $\langle [a_1, b_1] \rangle$ and $\langle a^{q^{r_\alpha}} \rangle$, and $|Z(G)| = q^m$, where $m = \max\{l, r_1, n_\alpha - r_\alpha\}$. Consequently $x^{q^m} \in Z(G)$ for all $x \in G$. We can then consider U as a Z_{q^m}-module. Define the following Z_{q^m}-bilinear form on U as follows

$$(\cdot, \cdot) : U \times U \to Z_{q^m} ,$$

for all $x, y \in G$, $(\bar{x}, \bar{y}) = \lambda$ where $[x, y] = z^\lambda$ and z is the generator of $Z(G)$ given in Lemma 4.2.9. Clearly λ is uniquely determined modulo q^m. Since G is of class 2, $[x, y_1 y_2] = [x, y_1][x, y_2]$ for all $x, y_1, y_2 \in G$, and hence the bilinearity of $(\cdot, \cdot)$ follows easily. That $(\cdot, \cdot)$ is an alternating form is evident. To see that it is non-degenerate, suppose $(\bar{x}, \bar{y}) = 0$ for all $\bar{y} \in U$. Then $[x, y] = 1$ for all $y \in G$ and so $x \in Z(G)$, that is, $\bar{x} = 0$. Thus U is a non-degenerate symplectic module over Z_{q^m}.

We single out the following sets of elements of G whose significance will be apparent later on:

$$A_i = \left\{ x \in G : x^{q^{r_i}} = a_i^{q^{r_i}} \right\} , \quad i = 1, \ldots, \alpha ,$$

$$B_i = \left\{ x \in G : x^{q_i^{r_i}} = 1 \right\}, \quad i = 1, \ldots, \alpha ,$$

$$D_i = \left\{ x \in G : x^{q^i} = 1 \right\}, \quad i = 1, \ldots, l .$$

We will be interested in a certain subgroup of the group $Sp(U)$ of isometries of U. This subgroup which we denote by $QSp(U)$ consists of all the isometries $\bar{\varphi}$ of U such that $\bar{a}_i\bar{\varphi} = \bar{x}_i$, $\bar{b}_i\bar{\varphi} = \bar{y}_i$ where $x_i \in A_i$, $y_i \in B_i$, $i = 1, \ldots, \alpha$, $\bar{a}_{jk}\bar{\varphi} = \bar{x}_{jk}$, $\bar{b}_{jk}\bar{\varphi} = \bar{y}_{jk}$ where $x_{jk}, y_{jk} \in D_j$, $k = 1, \ldots, \varepsilon_j$, $1 \leq j \leq l$. The following theorem shows that the set of such isometries is, in fact, a group.

4.2.2 THEOREM. $QSp(U) \cong \mathrm{aut}_Z G/\mathrm{inn}\, G$.

Proof. For every $\varphi \in \mathrm{aut}_Z G$, let $\bar{\varphi}$ be the induced automorphism of $G/Z(G)$, that is, $\bar{\bar{x}\bar{\varphi}} = \overline{x\varphi}$ for all $x \in G$. This is well-defined. Suppose $(\bar{\bar{x}\bar{\varphi}}, \bar{\bar{y}\bar{\varphi}}) = \lambda$ where $[x\varphi, y\varphi] = z^\lambda$. Then $[x, y] = [x, y]\varphi = [x\varphi, y\varphi] = z^\lambda$, and so $(\bar{x}, \bar{y}) = (\bar{\bar{x}\bar{\varphi}}, \bar{\bar{y}\bar{\varphi}})$; hence $\bar{\varphi} \in Sp(U)$. Moreover if $a_i\varphi = x_i$, $i = 1, \ldots, \alpha$, then $x_i^{q_i^{r_i}} = a_i^{q_i^{r_i}}\varphi = a_i^{q_i^{r_i}}$ since $a_i^{q_i^{r_i}} \in Z(G)$ and φ acts trivially on $Z(G)$, so that $x_i \in A_i$. It can be easily verified that $b_i\varphi \in B_i$, $i = 1, \ldots, \alpha$, and that $a_{jk}\varphi, b_{jk}\varphi \in D_j$, $k = 1, \ldots, \varepsilon_j$, $1 \leq j \leq l$. In other words, $\bar{\varphi} \in QSp(U)$.

Consider the mapping

$$\Gamma : \mathrm{aut}_Z G \to QSp(U),$$

$$\varphi \mapsto \bar{\varphi} .$$

It is clear that Γ is a homomorphism. We show that it is onto. Let $\bar{\varphi} \in QSp(U)$ and let $\bar{a}_i\bar{\varphi} = \bar{x}_i$, $\bar{b}_i\bar{\varphi} = \bar{y}_i$, $\bar{a}_{jk}\bar{\varphi} = \bar{x}_{jk}$, $\bar{b}_{jk}\bar{\varphi} = \bar{y}_{jk}$, $i = 1, \ldots, \alpha$, $k = 1, \ldots, \varepsilon_j$, $1 \leq j \leq l$. Define the mapping φ on the set of canonic generators of G by $a_i\varphi = x_i$, $b_i\varphi = y_i$, $a_{jk}\varphi = x_{jk}$, $b_{jk}\varphi = y_{jk}$. We define φ on an arbitrary element of G by linearity. If we can show that every defining relation in G

remains a valid relation under φ, then von Dyck's Theorem (Corollary to Theorem 21, p. 52, B.H. Neumann [19]) tells us that φ is a homomorphism. First note that φ is trivial on $Z(G)$. For $Z(G)$ is generated by $a_\alpha^{q^{r_\alpha}}$ or $[a_1, b_1]$ or $[a_{l1}, b_{l1}]$, by Lemma 4.2.9. In the first case, $a_\alpha^{q^{r_\alpha}}\varphi = x_\alpha^{q^{r_\alpha}} = a_\alpha^{q^{r_\alpha}}$ since $x_\alpha \in A_\alpha$, while in the other two cases φ fixes the commutators because $\bar{\varphi}$ is an isometry. Finally the defining relations in G are of the form $a_i^{q^{n_i}} = b_i^{q^{r_i}} = 1$, $a_i^{q^{n_i - r_i}} = [a_i, b_i]$, $a_i^{q^{r_i}} = [a_i, b_i]^{q^{2r_i - n_i}}$, $[a_i, a_j] = [a_i, b_j] = [b_i, b_j] = 1$, $i \neq j$, etc. By the preceding remarks and the fact that $y_i \in B_i$, $x_{jk}, y_{jk} \in D_j$, the defining relations in G remain valid relations under the mapping φ. So φ is indeed a homomorphism. The images of the generators of G generate G modulo $Z(G) \leq \Phi(G)$, and hence generate G. Therefore φ is onto and so must be an automorphism because G is finite. Thus $\varphi \in \mathrm{aut}_Z G$ and clearly $\varphi\Gamma = \bar{\varphi}$.

For every $\varphi \in \mathrm{inn}\, G$, there is some $y \in G$ such that $x\varphi = x^y = x[x, y]$ for all $x \in G$. Hence $\varphi \in \mathrm{aut}_Z G$ and $\varphi \in \ker \Gamma$, that is, $\mathrm{inn}\, G \leq \ker \Gamma$. Now $\ker \Gamma$ consists of precisely the elements φ of the form $a_i\varphi = a_i z^{\nu_i}$, $b_i\varphi = b_i z^{\tau_i}$ where $\nu_i \equiv 0 \equiv \tau_i \pmod{q^{m-r_i}}$, $a_{jk}\varphi = a_{jk} z^{\nu_{jk}}$, $b_{jk}\varphi = b_{jk} z^{\tau_{jk}}$ where $\nu_{jk} \equiv 0 \equiv \tau_{jk} \pmod{q^{m-r}}$, for $i = 1, \ldots, \alpha$, $k = 1, \ldots, \varepsilon_j$, $1 \leq j \leq l$; Lemmas 4.2.11-4.2.17. Consequently $|\ker \Gamma| = |G/Z(G)| = |\mathrm{inn}\, G|$, and so $\ker \Gamma = \mathrm{inn}\, G$. //

Define the following submodule of U,

$$U(\delta_1, \ldots, \delta_h) = \langle \bar{a}_i, \bar{b}_i, \bar{a}_{jk}, \bar{b}_{jk} : i = 1, \ldots, \alpha,\ k = 1, \ldots, \delta_j,\ 1 \leq j \leq h \rangle,$$

where $1 \leq h \leq l$, $0 \leq \delta_j \leq \varepsilon_j$ for $1 \leq j \leq h$, $\delta_h > 0$. This is generated by all but certain pairs $[\bar{a}_{jk}, \bar{b}_{jk}]$ of the generators of

U . (We will denote an ordered pair of elements of the module U by $[\bar{x}, \bar{y}]$; there is no confusion between this notation and the commutator $[x, y]$ of G .) Let us denote this submodule by V for simplicity and define the subgroup $QSp(V)$ of $Sp(V)$ by

$$QSp(V) = \{\bar{\psi} \in Sp(V) : \bar{\psi} = \bar{\varphi}|_V \text{ for some } \bar{\varphi} \in QSp(U)\} .$$

It consists of the restrictions to V of isometries in $QSp(U)$ which yield isometries of V . If we wish to emphasize the module V , we will write $QSp(\delta_1, \ldots, \delta_h)$. We now introduce the notion of a quasi-hyperbolic pair of V . An ordered pair $[\bar{x}, \bar{y}]$ of elements of V is called a *quasi-hyperbolic pair* (or simply qhp) of V if $x, y \in D_h$ and $(\bar{x}, \bar{y}) = q^{m-h}$. We denote the number of qph's of V by $\tilde{\omega}(V)$ or $\tilde{\omega}(\delta_1, \ldots, \delta_h)$. Its role is analogous to that of a hyperbolic pair in 4.1 as the next lemma indicates.

4.2.3 LEMMA. *Let* $V = U(\delta_1, \ldots, \delta_h)$, $\delta_h > 0$. *Then* $QSp(V)$ *acts transitively on the qhp's of* V .

Proof. Let $[\bar{x}, \bar{y}]$ be a qhp of V . By Lemma 4.2.27, there exists $\bar{\psi} \in QSp(V)$ such that $\bar{a}_{h1}\bar{\psi} = \bar{x}$. $\bar{b}_{h1}\bar{\psi} = \bar{y}$. For every $\bar{\varphi} \in QSp(V)$, $\bar{x}\bar{\varphi} = \bar{a}_{h1}\bar{\psi}\bar{\varphi}$, $\bar{y}\bar{\varphi} = \bar{b}_{h1}\bar{\psi}\bar{\varphi}$. Since $\bar{\psi}\bar{\varphi}$ clearly belongs to $QSp(V)$, $x\varphi, y\varphi \in D_h$, and $(\bar{x}\bar{\varphi}, \bar{y}\bar{\varphi}) = q^{m-h}$. In other words, $[\bar{x}\bar{\varphi}, \bar{y}\bar{\varphi}]$ is a qhp of V .

Suppose now $[\bar{x}', \bar{y}']$ is another qhp of V . Then there exists $\bar{\psi}' \in QSp(V)$ such that $\bar{a}_{h1}\bar{\psi}' = \bar{x}'$, $\bar{b}_{h1}\bar{\psi}' = \bar{y}'$. Put $\bar{\psi}_0 = \bar{\psi}^{-1}\bar{\psi}'$. Then $\bar{\psi}_0 \in QSp(V)$ and $\bar{x}\bar{\psi}_0 = \bar{x}'$, $\bar{y}\bar{\psi}_0 = \bar{y}'$. Hence the action of $QSp(V)$ given by $\bar{\varphi} : [\bar{x}, \bar{y}] \mapsto [\bar{x}\bar{\varphi}, \bar{y}\bar{\varphi}]$ is transitive. //

We also need to consider the submodule of U defined by $U^t = \langle \bar{a}_i, \bar{b}_i : i = t, t+1, \ldots, \alpha \rangle$, $1 \le t \le \alpha$. Again we introduce the corresponding subgroup $QSp(U^t)$ of $Sp(U^t)$ given by

$$QSp(U^t) = \left\{\bar{\psi} \in Sp(U^t) : \bar{\psi} = \bar{\varphi}|_{U^t} \text{ for some } \bar{\varphi} \in QSp(U)\right\} ,$$

which consists of the restrictions to U^t of isometries in $QSp(U)$

which yield isometries of U^t. Likewise we define a *quasi-hyperbolic pair* (or qhp) of U^t as an ordered pair $[\bar{x}, \bar{y}]$ of elements of U^t such that $x \in A_t$, $y \in B_t$ and $(\bar{x}, \bar{y}) = q^{m-r_t}$. We denote the number of qhp's of U^t by $\tilde{\omega}_t$. Analogous to Lemma 4.2.3 is

4.2.4 LEMMA. *Let* $1 \leq t \leq \alpha$. *Then* $QSp(U^t)$ *acts transitively on the qhp's of* U^t.

Proof. Since the proof is similar to that of Lemma 4.2.3, we will only outline the proof. Let $[\bar{x}, \bar{y}]$ be a qhp of U^t. By Lemma 4.2.28, there exists $\bar{\psi} \in QSp(U^t)$ such that $\bar{a}_t\bar{\psi} = \bar{x}$, $\bar{b}_t\bar{\psi} = \bar{y}$, and so $[\bar{x}\bar{\varphi}, \bar{y}\bar{\varphi}]$ is a qhp of U^t for every $\bar{\varphi} \in QSp(U^t)$. If $[\bar{x}', \bar{y}']$ is another qhp of U^t, then there exists $\bar{\psi}' \in QSp(U^t)$ such that $\bar{a}_t\bar{\psi}' = \bar{x}'$, $\bar{b}_t\bar{\psi}' = \bar{y}'$. Therefore $\bar{\psi}_0 = \bar{\psi}^{-1}\bar{\psi}' \in QSp(U^t)$ and $\bar{x}\bar{\psi}_0 = \bar{x}'$, $\bar{y}\bar{\psi}_0 = \bar{y}'$. The action of $QSp(U^t)$, $\bar{\varphi} : [\bar{x}, \bar{y}] \mapsto [\bar{x}\bar{\varphi}, \bar{y}\bar{\varphi}]$, is then transitive. //

We can now reduce the calculation of $|QSp(U)|$ to an enumeration of qhp's (*cf.* Lemma 4.1.14).

4.2.5 LEMMA. $|QSp(U)| = \tilde{\omega}_1 \ldots \tilde{\omega}_\alpha \cdot \prod_{i=1}^{d} \prod_{j=1}^{\varepsilon_i} \tilde{\omega}(\varepsilon_1, \ldots, \varepsilon_{i-1}, j)$.

Proof. Write $\bar{a} = \bar{a}_{l\varepsilon_l}$, $\bar{b} = \bar{b}_{l\varepsilon_l}$. Then $[\bar{a}, \bar{b}]$ is clearly a qhp of U. Let $S = \{\bar{\varphi} \in QSp(U) : \bar{a}\bar{\varphi} = \bar{a}, \ \bar{b}\bar{\varphi} = \bar{b}\}$. Then $S \cong QSp(\varepsilon_1, \ldots, \varepsilon_{l-1}, \varepsilon_l - 1)$ by Lemma 4.2.19. Since $QSp(U)$ acts transitively on the qhp's of U by Lemma 4.2.3, we have

$$|QSp(U)| = |S| . \tilde{\omega}(U) ,$$

or

$$|QSp(\varepsilon_1, \ldots, \varepsilon_l)| = |QSp(\varepsilon_1, \ldots, \varepsilon_{l-1}, \varepsilon_l - 1)| . \tilde{\omega}(\varepsilon_1, \ldots, \varepsilon_l) .$$

By the same argument together with Lemma 4.2.21,

$$|QSp(1)| = |QSp(U^1)| . \tilde{\omega}(1) .$$

Hence the above recurrence relation gives that

$$|QSp(\varepsilon_1, \ldots, \varepsilon_l)| = |QSp(U^1)| \cdot \prod_{i=1}^{l} \prod_{j=1}^{\varepsilon_i} \tilde{\omega}(\varepsilon_1, \ldots, \varepsilon_{i-1}, j) .$$

Let $1 \leq t < \alpha$. By Lemma 4.2.4, $QSp(U^t)$ acts transitively on the qhp's of U^t. Clearly $[\bar{a}_t, \bar{b}_t]$ is a qhp of U^t. Let $T = \{\bar{\varphi} \in QSp(U^t) : \bar{a}_t\bar{\varphi} = \bar{a}_t, \ \bar{b}_t\bar{\varphi} = \bar{b}_t\}$. Then by Lemma 4.2.23, $T = QSp(U^{t+1})$. Since $QSp(U^t)$ acts transitively on the qhp's of U^t by Lemma 4.2.4, we have

$$|QSp(U^t)| = |QSp(U^{t+1})| . \tilde{\omega}_t .$$

Let $\bar{\varphi} : U^\alpha \to U^\alpha$ with $\bar{a}_\alpha\bar{\varphi} = \bar{x}$, $\bar{b}_\alpha\bar{\varphi} = \bar{y}$ where $\bar{x}, \bar{y} \in U^\alpha = \bar{a}_\alpha, \bar{b}_\alpha$. It is then clear that $\bar{\varphi} \in QSp(U^\alpha)$ if and only if $[\bar{x}, \bar{y}]$ is a qhp of U^α. Hence $|QSp(U^\alpha)| = \tilde{\omega}_\alpha$ and so

$$|QSp(U^1)| = \tilde{\omega}_1 \ldots \tilde{\omega}_\alpha . \qquad //$$

In this section it will be convenient to fix the following notations:

$$n_0 = n_1, \quad r_0 = l, \quad n_{\alpha+1} = m = \max\{l, r_1, n_\alpha - r_\alpha\}, \quad r_{\alpha+1} = 1,$$

$$I_\beta = \{i : r_{\beta+1} \leq i \leq n_{\beta+1} - n_\beta + r_\beta\}, \quad 0 \leq \beta \leq \alpha,$$

$$J_\beta = \{i : n_{\beta+1} - n_\beta + r_\beta < i < r_\beta\}, \quad 1 \leq \beta \leq \alpha,$$

$$s_i = 2 \sum_{k=\beta+1}^{\alpha} r_k + \begin{cases} m - n_{\beta+1} & \text{if } i \in I_\beta, \ 0 \leq \beta \leq \alpha, \\ m - n_\beta + r_\beta & \text{if } i \in J_\beta, \ 1 \leq \beta \leq \alpha, \end{cases}$$

$$t_i = \begin{cases} 2\beta & \text{if } i \in I_\beta, \ 0 \leq \beta \leq \alpha, \\ 2\beta - 1 & \text{if } i \in J_\beta, \ 1 \leq \beta \leq \alpha. \end{cases}$$

Note that the I_β and J_β are disjoint sets of positive integers whose union is the set of integers $\{i : 1 \leq i \leq l\}$. This is easily checked by considering the various possible values of I_α. Also I_α

is empty or non-empty according as $m = n_\alpha - r_\alpha$ or $m > n_\alpha - r_\alpha$, and I_0 is empty or non-empty according as $r_1 > l$ or $r_1 \leq l$.

4.2.6 THEOREM. *With the above notations,*

$$\log_q |QSp(U)| = 2\alpha m + 4 \sum_{i=1}^{\alpha} \sum_{j=i}^{\alpha} r_j - \sum_{i=1}^{\alpha} r_i - 2 \sum_{i=1}^{\alpha} n_i + 2 \sum_{i=1}^{l} (s_i + it_i)\varepsilon_i + \log_q |Sp(\varepsilon_1, \ldots, \varepsilon_l)| ,$$

where

$$\log_q |Sp(\varepsilon_1, \ldots, \varepsilon_l)| = \sum_{i=1}^{l} \left\{(2i-1)\varepsilon_i^2 + (i-1)\varepsilon_i\right\} + 4 \sum_{i=1}^{l-1} \sum_{j=1}^{i} j\varepsilon_j\varepsilon_{i+1} + \sum_{i=1}^{l} \sum_{j=1}^{\varepsilon_i} \log_q (q^{2j}-1) .$$

Proof. Substitute the expressions from Lemmas 4.2.31, 4.2.32 into the formula of Lemma 4.2.5 and use Lemma 4.1.14. The expression for $|Sp(\varepsilon_1, \ldots, \varepsilon_l)|$ is obtained by substituting $\alpha = l$, $n_i = \varepsilon_{l-i+1}$ into the formula of Theorem 4.1.17 and rewriting the expression. //

So far we have only considered the case when $r_\alpha > 0$. In the case when G has the canonic form

$$G = Q(n_1, r_1) \ldots Q(n_\alpha, r_\alpha) Q(n_{\alpha+1}, 0) Q(l)^{\varepsilon_l} \ldots Q(1)^{\varepsilon_1} ,$$

where $\alpha \geq 1$, $r_\alpha > 0$, $\varepsilon_l > 0$, we have $Z(G) = Q(n_{\alpha+1}, 0)$, $|Z(G)| = q^{n_{\alpha+1}}$. It is not difficult to check that the same procedure described above carries through with obvious modifications (where necessary) in the details of the proofs and with the interpretation that $m = n_{\alpha+1}$ only. The details given below can also be checked to be true with only this change in notation. Thus in this case, Theorem 4.2.6 is still true provided we interprete $m = n_{\alpha+1}$.

In actual fact, Theorem 4.2.6 holds whether $r_\alpha > 0$ or $r_\alpha = 0$. Suppose that $r_\alpha = 0$. Then by the above remarks, we have for the

corresponding non-degenerate symplectic module U over Z_{q^m}, where clearly $m = n_\alpha = \max\{l, r_1, n_\alpha - r_\alpha\}$ since $n_\alpha > l$, $n_\alpha > r_1$ by definition of the canonic form,

$$\log_q |QSp(U)| = 2(\alpha-1)n_\alpha + 4 \sum_{i=1}^{\alpha-1} \sum_{j=i}^{\alpha-1} r_j - \sum_{i=1}^{\alpha-1} r_i - 2 \sum_{i=1}^{\alpha-1} n_i + 2 \sum_{i=1}^{l} (s_i + it_i)\varepsilon_i + \log_q |Sp(\varepsilon_1, \ldots, \varepsilon_l)| ,$$

which can be written in the expression of Theorem 4.2.6 with the same interpretation of the symbols.

We can even say more. If $\alpha = 0$, then the same method shows that $QSp(U) = Sp(U)$. With the usual interpretation of the fixed notations, we have $n_0 = n_1$, $r_0 = l$, $n_1 = m$, $r_1 = 1$, $I_0 = \{i : 1 \le i \le l\}$ and so $s_i = t_i = 0$, $i = 1, \ldots, l$. Consequently Theorem 4.2.6 is still true when $\alpha = 0$.

Moreover if $\varepsilon_i = 0$, $i = 1, \ldots, l$, that is, $G = Q(n_1, r_1) \ldots Q(n_\alpha, r_\alpha)$ with $\alpha \ge 1$, then $m = \max\{r_1, n_\alpha - r_\alpha\}$, and U and U_1 coincide, so that $|QSp(U)| = |QSp(U^1)|$. Omitting the easy details, we see that Theorem 4.2.6 also holds in this case if we interprete $|Sp(0)|$ to be 1.

Consequently if G has an arbitrary canonic form $G = Q(n_1, r_1) \ldots Q(n_\alpha, r_\alpha) Q(l)^{\varepsilon_l} \ldots Q(1)^{\varepsilon_1}$, then Lemma 4.2.1 and Theorem 4.2.2 tells us that

$$|\text{lin aut } G| = |QSp(U)| . |G/Z(G)| ,$$

where $|QSp(U)|$ is given by Theorem 4.2.6 with the same interpretation of the fixed notations and with the interpretation that $|Sp(0)| = 1$.

As a special case, we have

4.2.7 LEMMA. *If $k > l$, then*

$$\left|\text{lin aut}\left(Q(k, 0)Q(l)^{\varepsilon_l} \ldots Q(1)^{\varepsilon_1}\right)\right| = \left|\text{lin aut}\left(Q(l)^{\varepsilon_l} \ldots Q(1)^{\varepsilon_1}\right)\right| .$$

We now give the proofs of the lemmas assumed in the above

discussion of this section. We will use the notations of Chapter 2.

4.2.8 LEMMA. *Let* G *have the canonic decomposition*

$$G \cong Q(n_1, r_1) \ldots Q(n_\alpha, r_\alpha)Q(l)^{\varepsilon_l} \ldots Q(1)^{\varepsilon_1} .$$

Then there is a unique integer β, $0 \le \beta \le \alpha$, *such that* $Q(n_i, r_i)$ *is of Type* II *for* $i = 1, \ldots, \beta$, *and* $Q(n_i, r_i)$ *is of Type* I *for* $i = \beta+1, \ldots, \alpha$.

Proof. If all the $Q(n_i, r_i)$ are of either Type I of Type II, there is nothing to prove. So suppose not all the $Q(n_i, r_i)$ are of Type I or Type II. Next note that if $Q(n_j, r_j)$ is of Type I for some $1 \le j < \alpha$, then $Q(n_{j+1}, r_{j+1})$ is also of Type I. Otherwise we would have $2r_{j+1} > n_{j+1}$ implies that $r_{j+1} > n_{j+1}-r_{j+1} > n_j-r_j \ge r_j$: a contradiction. We now define β to be the smallest integer $1 \le \beta < \alpha$ for which $Q(n_{\beta+1}, r_{\beta+1})$ is of Type I. By the preceding remark, $Q(n_i, r_i)$ is of Type I for all $i = \beta+1, \ldots, \alpha$, and by the definition of β, $Q(n_i, r_i)$ is of Type II for all $i = 1, \ldots, \beta$. //

In the rest of this section G will be assumed to have the fixed canonic decomposition (unless stated otherwise)

$$G \cong Q(n_1, r_1) \ldots Q(n_\alpha, r_\alpha)Q(l)^{\varepsilon_l} \ldots Q(1)^{\varepsilon_1}$$

with $\alpha \ge 1$, $r_\alpha > 0$, $\varepsilon_l > 0$.

4.2.9 LEMMA. *Canonic generators,* a_i, b_i, a_{jk}, b_{jk}, $i = 1, \ldots, \alpha$, $k = 1, \ldots, \varepsilon_j$, $1 \le j \le l$, *of* G *can be chosen where*

$$Q(n_i, r_i) \cong \langle a_i, b_i \rangle , \quad i = 1, \ldots, \alpha ,$$

$$Q(j)^{\varepsilon_j} \cong \langle a_{jk}, b_{jk} : k = 1, \ldots, \varepsilon_j \rangle , \quad j = 1, \ldots, l ,$$

such that the following relations hold:

$$a_i^{q^{r_i}} = z^{q^{m-n_i+r_i}} , \quad i = 1, \ldots, \alpha ,$$

$$[a_i, b_i] = z^{q^{m-r_i}} , \quad i = 1, \ldots, \alpha ,$$

$$[a_{jk}, b_{jk}] = z^{q^{m-j}} , \quad k = 1, \ldots, \varepsilon_j , \quad 1 \le j \le l ,$$

where $m = \max\{l, r_1, n_\alpha - r_\alpha\}$, $Z(G) = \langle z \rangle$ *and* $|Z(G)| = q^m$.

Proof. Choose β to be the unique integer of Lemma 4.2.8. We consider three cases: (i) $\beta = 0$, (ii) $\beta = \alpha$, (iii) $0 < \beta < \alpha$. As the details are matters of routine, we will only give the details in Case (i).

(i) All the $Q(n_i, r_i)$ are of Type I. We have

$$|Z(Q(n_i, r_i))| = \left|\left\langle a_i^{q^{r_i}} \right\rangle\right| = q^{n_i - r_i} , \quad i = 1, \ldots, \alpha .$$

Since $n_\alpha - r_\alpha > \ldots > n_1 - r_1$, $|Z(G_*)| = q^{n_\alpha - r_\alpha}$. Also $|Z(G_0)| = q^l$.

(a) $l \ge n - r$. Then $Z(G) = Z(G_0) = \langle z \rangle$ where $z = [a_{l1}, b_{l1}]$. The amalgamation may be chosen such that $a_i^{q^{r_i}} = z^{q^{l-n_i+r_i}}$, $[a_{jk}, b_{jk}] = z^{q^{l-j}}$. Moreover $[a_i, b_i] = a_i^{q^{n_i-r_i}} = z^{q^{l-r_i}}$.

(b) $l < n_\alpha - r_\alpha$. Then $Z(G) = Z(G_*) = \langle z \rangle$ where $z = a_\alpha^{q^{r_\alpha}}$. We can then have $a_i^{q^{r_i}} = z^{q^{n_\alpha - r_\alpha - n_i + r_i}}$, $[a_{jk}, b_{jk}] = z^{q^{n_\alpha - r_\alpha - j}}$, and so $[a_i, b_i] = z^{q^{n_\alpha - r_\alpha - r_i}}$. Note that $n_\alpha - r_\alpha > \ldots > n_1 - r_1 \ge r_1$. //

Henceforth we will fix a set of canonic generators of G to satisfy the above lemma.

4.2.10 LEMMA. *Every element of* G *can be uniquely written in the form*

$$\left(\prod_{i=1}^{\alpha} a_i^{\lambda_i} b_i^{\mu_i}\right) c z^{\nu} , \quad 0 \le \nu < q^m , \quad 0 \le \lambda_i , \ \mu_i < q^{r_i} , \quad i = 1, \ldots, \alpha ,$$

where c *is of the form*

$$c = \prod_{j=1}^{l} \prod_{k=1}^{\varepsilon_j} a_{jk}^{\lambda_{jk}} b_{jk}^{\mu_{jk}} , \quad 0 \le \lambda_{jk} , \ \mu_{jk} < q^j ,$$

$$k = 1, \ldots, \varepsilon_j , \quad 1 \le j \le l .$$

Proof. By Lemma 4.2.9, every element of G can be written in the above form. To prove uniqueness, suppose $x \in G$ has two such forms

$$x = \left(\prod_{i=1}^{\alpha} a_i^{\lambda_i} b_i^{\mu_i}\right)\left(\prod_{j=1}^{l} \prod_{k=1}^{\varepsilon_j} a_{jk}^{\lambda_{jk}} b_{jk}^{\mu_{jk}}\right) z^{\nu}$$

$$= \left(\prod_{i=1}^{\alpha} a_i^{\rho_i} b_i^{\sigma_i}\right)\left(\prod_{j=1}^{l} \prod_{k=1}^{\varepsilon j} a_{jk}^{\rho_{jk}} b_{jk}^{\sigma_{jk}}\right) z^{\nu} .$$

Commuting with a_i, we get $[a_i, b_i]^{\mu_i} = [a_i, b_i]^{\sigma_i}$, $i = 1, \ldots, \alpha$, and hence $\mu_i = \sigma_i$, $i = 1, \ldots, \alpha$. Commuting with b_i, we have $[a_i, b_i]^{\lambda_i} = [a_i, b_i]^{\rho_i}$, $i = 1, \ldots, \alpha$, and hence $\lambda_i \equiv \rho_i \pmod{p^{r_i}}$. Since $0 \le \lambda_i , \ \rho_i < q^{r_i}$, we must have $\lambda_i = \rho_i$, $i = 1, \ldots, \alpha$. Finally commuting with b_{jk} and a_{jk}, we conclude that $\lambda_{jk} = \rho_{jk}$, $\mu_{jk} = \sigma_{jk}$, $k = 1, \ldots, \varepsilon_j$, $1 \le j \le l$. //

The following seven lemmas describe explicitly the sets A_i, B_i and D_i defined earlier (preceding Theorem 4.2.2).

4.2.11 LEMMA. *Let* $1 \le i \le \alpha$ *and* $x \in G$. *Then* $x \in A_i$ *if and only if*

$$x = \left(\prod_{j=1}^{i-1} a_j^{\lambda_j q^{r_j - r_i}} b_j^{\mu_j q^{r_j - r_i}}\right)\left(a_i^{1-\lambda^* + \lambda_i q^{n_i - n_{i+1}}} b_i^{\mu_i}\right) \times$$

$$\times \left(\prod_{j=i+1}^{\alpha} a_j^{-\lambda_{j-1} + \lambda_j q^{n_j - n_{j+1}}} b_j^{\mu_j}\right) c z^{\nu} ,$$

where

$$c^{q^{r_i}} = 1 , \quad n_{\alpha+1} = m ,$$

$$\lambda^* = \sum_{j=1}^{i-1} \lambda_j q^{n_i - n_j + r_j - r_i} ,$$

$$\lambda_\alpha + \nu \equiv 0 \pmod{q^{m-r_i}} .$$

Proof. Let $x = \left(\prod_{j=1}^{\alpha} a_j^{\lambda_j} b_j^{\mu_j} \right) c z^\nu$, where $c = \prod_{j=1}^{l} \prod_{k=1}^{\varepsilon_j} a_{jk}^{\lambda_{jk}} b_{jk}^{\mu_{jk}}$, from Lemma 4.2.10. Suppose $x \in A_i$. Then

$$a_i^{q^{r_i}} = \left(\prod_{j=1}^{i-1} a_j^{\lambda_j q^{r_i}} b_j^{\mu_j q^{r_i}} [b_j, a_j]^{\lambda_j \mu_j \binom{q^{r_i}}{2}} \right) \left(\prod_{j=i}^{\alpha} a_j^{\lambda_j q^{r_i}} \right) c^{q^{r_i}} z^{\nu q^{r_i}} ,$$

and $c^{q^{r_i}} = \prod_{j=r_i+1}^{l} \prod_{k=1}^{\varepsilon_i} a_{jk}^{\lambda_{jk} q^{r_i}} b_{jk}^{\mu_{jk} q^{r_i}} [b_{jk}, a_{jk}]^{\lambda_{jk}\mu_{jk}\binom{q^{r_i}}{2}}$.

Commuting with a_{jk} and b_{jk} , we have

$$1 = \left[a_{jk}, c^{q^{r_i}} \right] = \left[c^{q^{r_i}}, b_{jk} \right] ,$$

that is, $1 = [a_{jk}, b_{jk}]^{\lambda_{jk} q^{r_i}} = [a_{jk}, b_{jk}]^{\mu_{jk} q^{r_i}}$, $r_i < j \le l$.

Hence $\lambda_{jk} = \lambda'_{jk} q^{j-r_i}$, $\mu_{jk} = \mu'_{jk} a^{j-r_i}$, $r_i < j \le l$. Moreover

$\lambda_{jk}\mu_{jk}\binom{q^{r_i}}{2} = \frac{1}{2}(q^{r_i}-1)\lambda'_{jk}\mu'_{jk} q^{2j-r_i} \equiv 0 \pmod{q^j}$ since $j > r_i$. Thus

$c^{q^{r_i}} = 1$.

Commuting with a_j, b_j , $1 \le j < i$, we have

$$1 = [a_j, b_j]^{\lambda_j q^{r_i}} = [a_j, b_j]^{\mu_j q^{r_i}} .$$

Hence $\lambda_j = \lambda'_j q^{r_j - r_i}$, $\mu_j = \mu'_j q^{r_j - r_i}$, $1 \le j < i$, and

$\lambda_j \mu_j \begin{bmatrix} r_i \\ 2 \end{bmatrix}_q = \frac{1}{2}(q^{r_i} - 1)\lambda'_j \mu'_j q^{2r_j - r_i} \equiv 0 \pmod{q^{r_j}}$. Therefore

$$a_i^{q^{r_i}} = \left(\prod_{j=1}^{i-1} a_j^{\lambda'_j q^{r_j}} \right) \left(\prod_{j=i}^{\alpha} a_j^{\lambda_j q^{r_i}} \right) z^{\nu q^{r_i}} .$$

By Lemma 4.2.9, we have for $i \le j \le \alpha$,

$$a_i^{q^{r_i}} = \left(a_j^{q^{r_j}} \right)^{q^{r_i - r_j}} = z^{q^{m - n_j + r_i}} .$$

Hence

$$z^{q^{m-n_i+r_i}} = \left(\prod_{j=1}^{i-1} z^{\lambda'_j q^{m-n_j+r_j}} \right) \left(\prod_{j=1}^{\alpha} z^{\lambda_j q^{m-n_j+r_j}} \right) z^{\nu q^{r_i}} ,$$

that is,

$$q^{m-n_i+r_i} \equiv \sum_{j=1}^{i-1} \lambda'_j q^{m-n_j+r_j} + \sum_{j=i}^{\alpha} \lambda_j q^{m-n_j+r_j} + \nu q^{r_i} \pmod{q^m} .$$

Since

$$m - n_1 + r_1 > \ldots > m - n_{i-1} + r_{i-1} > m - n_i + r_i ,$$

$$m - n_i + r_i < \ldots < m - n_\alpha + r_i \le r_i ,$$

we get on dividing throughout by $q^{m-n_i+r_i}$,

$$1 \equiv \sum_{j=1}^{i-1} \lambda'_j q^{n_i - n_j + r_j - r_i} + \sum_{j=i}^{\alpha} \lambda_j q^{n_i - n_j} + \nu q^{n_i - m} \pmod{q^{n_i - r_i}} .$$

Denoting the first sum on the right by λ^* , we have

$$1 \equiv \lambda^* + \lambda_i \pmod{q^{n_i - n_{i+1}}} .$$

Write $\lambda^* + \lambda_i = 1 + \lambda'_i q^{n_i - n_{i+1}}$. Then

$$0 \equiv \lambda'_i q^{n_i - n_{i+1}} + \sum_{j=i+1}^{\alpha} \lambda_j q^{n_i - n_j} + \nu q^{n_i - m} \pmod{q^{n_i - r_i}} ,$$

or

$$0 \equiv \lambda_i' + \sum_{j=i+1}^{\alpha} \lambda_j q^{n_{i+1}-n_j} + \nu q^{n_{i+1}-m} \pmod{q^{n_{i+1}-r_i}}.$$

Hence $\lambda_i' + \lambda_{i+1} = \lambda_{i+1}' q^{n_{i+1}-n_{i+2}}$. Then

$$0 \equiv \lambda_{i+1}' + \sum_{j=i+2}^{\alpha} \lambda_j q^{n_{i+2}-n_j} + \nu q^{n_{i+2}-m} \pmod{q^{n_{i+2}-r_i}}.$$

Proceeding in this manner, we have for $i < k < \alpha$,

$$\lambda_{k-1}' + \lambda_k = \lambda_k' q^{n_k - n_{k+1}},$$

$$0 \equiv \lambda_k' + \sum_{j=k+1}^{\alpha} \lambda_j q^{n_{k+1}-n_j} + \nu q^{n_{k+1}-m} \pmod{q^{n_{k+1}-r_i}}.$$

In particular for $k = \alpha-1$, we have

$$\lambda_{\alpha-2}' + \lambda_{\alpha-1} = \lambda_{\alpha-1}' q^{n_{\alpha-1}-n_\alpha},$$

$$0 \equiv \lambda_{\alpha-1}' + \lambda_\alpha + \nu q^{n_\alpha - m} \pmod{q^{n_\alpha - r_i}},$$

so that

$$\lambda_{\alpha-1}' + \lambda_\alpha = \lambda_\alpha' q^{n_\alpha - m},$$

$$\lambda_\alpha' + \nu \equiv 0 \pmod{q^{m-r_i}}.$$

Thus

$$\lambda_i = 1 - \lambda^* + \lambda_i' q^{n_i - n_{i+1}},$$

$$\lambda_j = -\lambda_{j-1}' + \lambda_j' q^{n_j - n_{j+1}}, \quad i < j \le \alpha.$$

Suppressing the dashes, we have the required form. The converse is easily verified. //

4.2.12 LEMMA. *Let* $1 \le i \le \alpha$ *and* $x \in G$. *Then* $x \in B_i$ *if and only if*

$$x = \left(\prod_{j=1}^{i-1} a_j^{\lambda_j q^{r_j - r_i}} b_j^{\mu_j q^{r_j - r_i}}\right)\left(a_i^{-\lambda^* + \lambda_i q^{n_i - n_{i+1}}} b_i^{\mu_i}\right) \times$$

$$\times \left(\prod_{j \neq i+1}^{\alpha} a_j^{-\lambda_{j-1} + \lambda_j q^{n_j - n_{j+1}}} b_j^{\mu_j}\right) c z^{\nu},$$

where $c^{q^{r_i}} = 1$, $n_{\alpha+1} = m$,

$$\lambda^* = \sum_{j=1}^{i-1} \lambda_j q^{n_i - n_j + r_j - r_i},$$

$$\lambda_\alpha + \nu \equiv 0 \pmod{q^{m-r_i}}.$$

Proof. Similar to that of Lemma 4.2.11. //

4.2.13 LEMMA. *Suppose* $r_1 \leq l$. *Let* $i \in I_0$ *and* $x \in G$. *Then* $x \in D_i$ *if and only if*

$$x = \left(\prod_{j=1}^{\alpha} a_j^{-\lambda_{j-1} + \lambda_j q^{n_j - n_{j+1}}} b_j^{\mu_j}\right) c z^{\nu},$$

where $c^{q^i} = 1$, $\lambda_0 = 0$, $n_{\alpha+1} = m$, $\lambda_\alpha + \nu \equiv 0 \pmod{q^{m-i}}$.

Proof. Let $x = \left(\prod_{j=1}^{\alpha} a_j^{\lambda_j} b_j^{\mu_j}\right) c z^{\nu} \in D_i$. Then $x^{q^i} = 1$. As before, we have $c^{q^i} = 1$. Since $i \geq r_1$, we have

$$a_j^{q^i} = \left(a_j^{q^{r_j}}\right)^{q^{i-r_j}} = z^{q^{m-n_j+i}}, \quad j = 1, \ldots, \alpha.$$

Hence

$$1 = \left(\prod_{j=1}^{\alpha} z^{\lambda_j q^{m-n_j+i}}\right) z^{\nu q^i},$$

that is,

$$0 \equiv \sum_{j=1}^{\alpha} \lambda_j q^{m-n_j+i} + \nu q^i \pmod{q^m}.$$

Since $m-n_1+i < \ldots < m-n_\alpha+i \leq i$, we have on dividing by q^{m-n_1+i},

$$0 \equiv \sum_{j=1}^{\alpha} \lambda_j q^{n_1-n_j} + \nu q^{n_1-m} \pmod{q^{n_1-i}},$$

and hence $\lambda_1 \equiv 0 \pmod{q^{n_1-n_2}}$. Write $\lambda_1' = \lambda_1 a^{n_1-n_2}$. Substituting for λ_1 and dividing by $q^{n_1-n_2}$, we have

$$0 \equiv \lambda_1' + \sum_{j=2}^{\alpha} \lambda_j q^{n_2-n_j} + \nu q^{n_2-m} \pmod{q^{n_2-i}}.$$

Therefore $0 \equiv \lambda_1' + \lambda_2 \pmod{q^{n_2-n_3}}$. Write $\lambda_1' + \lambda_2 = \lambda_2' q^{n_2-n_3}$. Continuing in this manner, we obtain

$$\lambda_j = -\lambda_{j-1}' + \lambda_j' q^{n_j-n_{j+1}}, \quad j = 1, \ldots, \alpha,$$

where $\lambda_0 = 0$, $n_{\alpha+1} = m$, $\lambda_\alpha' + \nu \equiv 0 \pmod{q^{m-i}}$. Suppressing the dashes, we get the required result. Converse is easy. //

4.2.14 LEMMA. *Let* $i \in J_\beta$, $1 \leq \beta < \alpha$, *and* $x \in G$. *Then* $x \in D_i$ *if and only if*

$$x = \begin{pmatrix} \prod_{j=1}^{\beta-1} a_j^{r_j-i} q^{\lambda_j r_j - i} & \mu_j q^{r_j-i} \\ & b_j \end{pmatrix} \begin{pmatrix} a_\beta^{-\lambda^*+\lambda_\beta} q^{n_\beta-n_{\beta+1}} & \mu_\beta q^{r_\beta-i} \\ & b_\beta \end{pmatrix} \times$$

$$\times \begin{pmatrix} \prod_{j=\beta+1}^{\alpha} a_j^{-\lambda_{j-1}+\lambda_j} q^{n_j-n_{j+1}} & \mu_j \\ & b_j \end{pmatrix} cz^\nu,$$

where

$$c^{q^i} = 1, \quad n_{\alpha+1} = m,$$

$$\lambda^* = \sum_{j=1}^{\beta-1} \lambda_j q^{n_\beta-n_j+r_j-i},$$

$$\lambda_\alpha + \nu \equiv 0 \pmod{q^{m-i}}.$$

Proof. Let $x = \left(\prod_{j=1}^{\alpha} a_j^{\lambda_j} b_j^{\mu_j}\right) c z^\nu \in D_i$. Then $x^{q^i} = 1$, or

$$1 = \left(\prod_{j=1}^{\beta} a_j^{\lambda_j q^i} b_j^{\mu_j q^i} [b_j, a_j]^{\lambda_j \mu_j \binom{q^i}{2}}\right)\left(\prod_{j=\beta+1}^{\alpha} a_j^{\lambda_j q^i}\right) c^{q^i} z^{\nu q^i}$$

since $i > n_{\beta+1} - n_\beta + r_\beta > r_{\beta+1}$. As usual, we have $c^{q^i} = 1$, $\lambda_j = \lambda'_j q^{r_j - i}$, $\mu_j = \mu'_j q^{r_j - i}$, $j = 1, \ldots, \beta$. Hence

$$1 = \left(\prod_{j=1}^{\beta} a_j^{\lambda'_j q^{r_j}}\right)\left(\prod_{j=\beta+1}^{\alpha} a_j^{\lambda_j q^i}\right) z^{\nu q^i}$$

$$= \left(\prod_{j=1}^{\beta} z^{\lambda'_j q^{m-n_j+r_j}}\right)\left(\prod_{j=\beta+1}^{\alpha} z^{\lambda_j q^{m-n_j+i}}\right) z^{\nu q^i},$$

that is

$$0 \equiv \sum_{j=1}^{\beta} \lambda'_j q^{m-n_j+r_j} + \sum_{j=\beta+1}^{\alpha} \lambda_j q^{m-n_j+i} + \nu q^i \pmod{q^m}.$$

Since $m-n_1+r_1 > \ldots > m-n_\beta+r_\beta$,

$$m-n_\beta+r_\beta < m-n_{\beta+1}+i < \ldots < m-n_\alpha+i < i,$$

we can divide by $q^{m-n_\beta+r_\beta}$. We then have

$$0 \equiv \sum_{j=1}^{\beta} \lambda_j q^{n_\beta-n_j+r_j-r_\beta} + \sum_{j=\beta+1}^{\alpha} \lambda_j q^{n_\beta-n_j+i-r_\beta} + \nu q^{n_\beta-m+i-r_\beta} \pmod{q^{n_\beta-r_\beta}}.$$

Since $n_\beta-n_{\beta+1}+i-r_\beta < \ldots < n_\beta-n_\alpha+i-r_\beta < n_\beta-m+i-r_\beta$, we have

$$0 \equiv \sum_{j=1}^{\beta-1} \lambda'_j q^{n_\beta-n_j+r_j-r_\beta} + \lambda'_\beta \pmod{q^{n_\beta-n_{\beta+1}+i-r_\beta}}.$$

Denote the first sum by λ_0^*. Then

$$\lambda_0^* + \lambda'_\beta = \lambda''_\beta q^{n_\beta - n_{\beta+1} + i - r_\beta} ,$$

so that $\lambda_\beta = \lambda'_\beta q^{r_\beta - i} = -\lambda^* + \lambda''_\beta q^{n_\beta - n_{\beta+1}}$ where $\lambda^* = \lambda_0^* q^{r_\beta - i}$. Also

$$0 \equiv \lambda''_\beta q^{n_\beta - n_{\beta+1} + i - r_\beta} + \sum_{j=\beta+1}^{\alpha} \lambda_j q^{n_\beta - n_j + i - r_\beta} + \nu q^{n_\beta - m + i - r_\beta} \pmod{q^{n_\beta - r_\beta}}.$$

Dividing by $q^{n_\beta - n_{\beta+1} + i - r_\beta}$, we get

$$0 \equiv \lambda''_\beta + \sum_{j=\beta+1}^{\alpha} \lambda_j q^{n_{\beta+1} - n_j} + \nu q^{n_{\beta+1} - m} \pmod{q^{n_{\beta+1} - i}}.$$

Hence $0 \equiv \lambda''_\beta + \lambda_{\beta+1} \pmod{q^{n_{\beta+1} - n_{\beta+2}}}$. Write

$\lambda''_\beta + \lambda_{\beta+1} = \lambda'_{\beta+1} q^{n_{\beta+1} - n_{\beta+2}}$. Proceeding in this way, we obtain

$$\lambda_j = -\lambda'_{j-1} + \lambda'_j q^{n_j - n_{j+1}} , \quad \beta+1 < j \le \alpha ,$$

and $\lambda'_\alpha + \nu \equiv 0 \pmod{q^{m-i}}$. Suppressing the dashes, we get the required result. Converse is easy. //

4.2.15 LEMMA. *Let* $i \in I_\beta$, $1 \le \beta < \alpha$, *and* $x \in G$. *Then* $x \in D_i$ *if and only if*

$$x = \left(\prod_{j=1}^{\beta} a_j^{\lambda_j q^{r_j - i}} b_j^{\mu_j q^{r_j - i}} \right) \left(\prod_{j=\beta+1}^{\alpha} a_j^{-\lambda^*_{j-1} + \lambda^*_j q^{n_j - n_{j+1}}} b_j^{\mu_j} \right) c z^\nu$$

where

$$c^{q^i} = 1 , \quad n_{\alpha+1} = m ,$$

$$\lambda^*_\beta = \sum_{j=1}^{\beta} \lambda_j q^{n_{\beta+1} - n_j + r_j - i} ,$$

$$\lambda^*_\alpha + \nu \equiv 0 \pmod{q^{m-i}}.$$

Proof. Let $x = \left(\prod_{j=1}^{\alpha} a_j^{\lambda_j} b_j^{\mu_j} \right) c z^\nu \in D_i$. Then $x^{q^i} = 1$. As in

the proof of Lemma 4.2.14, we have $c^{q^i} = 1$, $\lambda_j = \lambda'_j q^{r_j - i}$,

$\mu_j = \mu'_j q^{r_j - i}$, $j = 1, \ldots, \beta$, and

$$0 \equiv \sum_{j=1}^{\beta} \lambda'_j q^{m-n_j+r_j} + \sum_{j=\beta+1}^{\alpha} \lambda_j q^{m-n_j+i} + \nu q^i \pmod{q^m}.$$

Now

$$m-n_1+r_1 > \ldots > m-n_\beta+r_\beta \geq m-n_{\beta+1}+i ,$$

$$m-n_{\beta+1}+i < \ldots < m-n_\alpha+i .$$

Dividing by $q^{m-n_{\beta+1}+i}$, we get

$$0 \equiv \sum_{j=1}^{\beta} \lambda'_j q^{n_{\beta+1}-n_j+r_j-i} + \sum_{j=\beta+1}^{\alpha} \lambda_j q^{n_{\beta+1}-n_j} + \nu q^{n_{\beta+1}-m} \pmod{q^{n_{\beta+1}-i}}.$$

Denoting the first sum by λ^*_β , we have

$$0 \equiv \lambda^*_\beta + \lambda_{\beta+1} \pmod{q^{n_{\beta+1}-n_{\beta+2}}}.$$

Write $\lambda^*_\beta + \lambda_{\beta+1} = \lambda^*_{\beta+1} q^{n_{\beta+1}-n_{\beta+2}}$. In this way, we have

$\lambda_j = -\lambda^*_{j-1} + \lambda^*_j q^{n_j - n_{j+1}}$, $j = \beta+1, \ldots, \alpha$, and $n_{\alpha+1} = m$,

$\lambda^*_\alpha + \nu \equiv 0 \pmod{q^{m-i}}$. Converse is easy. //

4.2.16 LEMMA. *Suppose that* $m-n_\alpha+r_\alpha > 0$. *Let* $i \in I_\alpha$ *and* $x \in G$. *Then* $x \in D_i$ *if and only if*

$$x = \left(\prod_{j=1}^{\alpha} a_j^{\lambda_j q^{r_j - i}} b_j^{\mu_j q^{r_j - i}} \right) c z^\nu ,$$

where $c^{q^i} = 1$, $\sum_{j=1}^{\alpha} \lambda_j q^{m-n_j+r_j-i} + \nu \equiv 0 \pmod{q^{m-i}}$.

Proof. Let $x = \left(\prod_{j=1}^{\alpha} a_j^{\lambda_j} b_j^{\mu_j} \right) c z^\nu \in D_i$. Then $x^{q^i} = 1$. In the usual manner, we get

$$c^{q^i} = 1 , \quad \lambda_j = \lambda'_j q^{r_j - i} , \quad \mu_j = \mu'_j q^{r_j - i} , \quad j = 1, \ldots, \alpha .$$

Thus

$$1 = \left(\prod_{j=1}^{\alpha} a_j^{\lambda'_j q^{r_j}} \right) z^{\nu q^i} = \left(\prod_{j=1}^{\alpha} z^{\lambda'_j q^{m-n_j+r_j}} \right) z^{\nu q^i} ,$$

that is, $0 \equiv \sum_{j=1}^{\alpha} \lambda'_j q^{m-n_j+r_j} + \nu q^i \pmod{q^m}$. Since

$i \le m-n_\alpha+r_\alpha < \ldots < m-n_1+r_1$, we have

$$0 \equiv \sum_{j=1}^{\alpha} \lambda'_j q^{m-n_j+r_j-i} + \nu \pmod{q^{m-i}} .$$

Converse is easy. //

4.2.17 LEMMA. *Let* $i \in J_\alpha$ *and let* $1 \le \gamma \le \alpha$ *be such that*

$$m-n_1+r_1 > \ldots > m-n_{\gamma-1}+r_{\gamma-1} \ge i > m-n_\gamma+r_\gamma > \ldots > m-n_\alpha+r_\alpha .$$

Let $x \in G$. *Then* $x \in D_i$ *if and only if*

$$x = \left(\prod_{j=1}^{\alpha-1} a_j^{\lambda_j q^{r_j-i}} b_j^{\mu_j q^{r_j-i}} \right) \left(a_\alpha^{-\lambda^* + \lambda_\alpha q^{n_\alpha - m}} b_\alpha^{\mu_\alpha q^{r_\alpha - i}} \right) c z^\nu ,$$

where $c^{q^i} = 1$, $\lambda^* = \sum_{j=\gamma}^{\alpha-1} \lambda_j q^{n_\alpha - n_j + r_j - i}$, *and*

$$\sum_{j=1}^{\gamma-1} \lambda_j q^{m-n_j+r_j-i} + \lambda_\alpha + \nu \equiv 0 \pmod{q^{m-i}} .$$

Proof. Let $x = \left(\prod_{j=1}^{\alpha} a_j^{\lambda_j} b_j^{\mu_j} \right) c z^\nu \in D_i$. As usual, we have

$c^{q^i} = 1$, $\lambda_j = \lambda'_j q^{r_j-i}$, $\mu_j = \mu'_j q^{r_j-i}$, $j = 1, \ldots, \alpha$, and

$$0 \equiv \sum_{j=1}^{\alpha} \lambda'_j q^{m-n_j+r_j} + \nu q^i \pmod{q^m} .$$

Dividing by $q^{m-n_\alpha+r_\alpha}$, we have

$$0 \equiv \sum_{j=1}^{\alpha} \lambda'_j q^{n_\alpha - n_j + r_j - r_\alpha} + \nu q^{i-m+n_\alpha - r_\alpha} \pmod{q^{n_\alpha - r_\alpha}}.$$

If $\gamma = \alpha$, then $i-m+n_\alpha - r_\alpha \leq n_\alpha - n_{\alpha-1} + r_{\alpha-1} - r_\alpha$, and hence

$$\lambda'_\alpha \equiv 0 \pmod{q^{i-m+n_\alpha - r_\alpha}}.$$

Write $\lambda'_\alpha = \lambda''_\alpha q^{i-m+n_\alpha - r_\alpha}$, so that $\lambda_\alpha = \lambda'_\alpha q^{r_\alpha - i} = \lambda''_\alpha q^{n_\alpha - m}$, and

$$0 \equiv \sum_{j=1}^{\alpha-1} \lambda'_j q^{m-n_j+r_j-i} + \lambda''_\alpha + \nu \pmod{q^{m-i}}.$$

In this case $\lambda^* = 0$.

So suppose $\gamma < \alpha$. Then $n_\alpha - n_{\alpha-1} + r_{\alpha-1} - r_\alpha < i-m+n_\alpha - r_\alpha$, and hence $\lambda'_\alpha \equiv 0 \pmod{q^{n_\alpha - n_{\alpha-1} + r_{\alpha-1} - r_\alpha}}$. Write $\lambda'_\alpha = \lambda''_\alpha q^{n_\alpha - n_{\alpha-1} + r_{\alpha-1} - r_\alpha}$. Therefore

$$0 \equiv \sum_{j=1}^{\alpha-1} \lambda'_j q^{n_\alpha - n_j + r_j - r_\alpha} + \lambda''_\alpha q^{n_\alpha - n_{\alpha-1} + r_{\alpha-1} - r_\alpha} + \nu q^{i-m+n_\alpha - r_\alpha} \pmod{q^{n_\alpha - r_\alpha}}.$$

Dividing by $q^{n_\alpha - n_{\alpha-1} + r_{\alpha-1} - r_\alpha}$, we get

$$0 \equiv \sum_{j=1}^{\alpha-2} \lambda'_j q^{n_{\alpha-1} - n_j + r_j - r_{\alpha-1}} + \left(\lambda'_{\alpha-1} + \lambda''_\alpha\right) + \nu q^{i-m+n_{\alpha-1} - r_{\alpha-1}} \pmod{q^{n_{\alpha-1} - r_{\alpha-1}}}.$$

If $\gamma = \alpha-1$, then $\lambda'_{\alpha-1} + \lambda''_\alpha = \lambda'''_\alpha q^{i-m+n_{\alpha-1} - r_{\alpha-1}}$, and the whole process stops on dividing by $q^{i-m+n_{\alpha-1} - r_{\alpha-1}}$. However if $\gamma < \alpha-1$, we continue the process. In general, for $2 \leq k \leq \alpha-\gamma$, we have

$$\lambda'_{\alpha-k+1} + \lambda^{(k)}_\alpha = \lambda^{(k+1)}_\alpha q^{n_{\alpha-k+1} - n_{\alpha-k} + r_{\alpha-k} - r_{\alpha-k+1}},$$

$$0 \equiv \sum_{j=1}^{\alpha-k-1} \lambda'_j q^{n_{\alpha-k} - n_j + r_j - r_{\alpha-k}} + \lambda'_{\alpha-k} + \lambda^{(k+1)}_\alpha + \nu q^{i-m+n_{\alpha-k} - r_{\alpha-k}} \pmod{q^{n_{\alpha-k} - r_{\alpha-k}}}.$$

In particular, for $k = \alpha-\gamma$ we have

$$\lambda'_{\gamma+1} + \lambda_\alpha^{(\alpha-\gamma)} = \lambda_\alpha^{(\alpha-\gamma+1)} q^{n_{\gamma+1}-n_\gamma+r_\gamma-r_{\gamma+1}} ,$$

$$0 \equiv \sum_{j=1}^{\gamma-1} \lambda'_j q^{n_\gamma-n_j+r_j-r_\gamma} + \lambda'_\gamma + \lambda_\alpha^{(\alpha-\gamma+1)} + \nu q^{i-m+n_\gamma-r_\gamma} \pmod{q^{n_\gamma-r_\gamma}} .$$

Now $n_\gamma-n_{\gamma-1}+r_{\gamma-1}-r_\gamma \geq i-m+n_\gamma-r_\gamma$. Hence

$$\lambda'_\gamma + \lambda_\alpha^{(\alpha-\gamma+1)} = \lambda_\alpha^{(\alpha-\gamma+2)} q^{i-m+n_\gamma-r_\gamma} .$$

Dividing by $q^{i-m+n_\gamma-r_\gamma}$, we have

$$0 \equiv \sum_{j=1}^{\gamma-1} \lambda'_j q^{m-n_j+r_j-i} + \lambda_\alpha^{(\alpha-\gamma+2)} + \nu \pmod{q^{m-i}} .$$

Moreover

$$\lambda_\alpha = \lambda'_\alpha q^{r_\alpha-i} = \lambda''_\alpha q^{n_\alpha-n_{\alpha-1}+r_{\alpha-1}-i}$$

$$= \left(-\lambda'_{\alpha-1}+\lambda'''_\alpha q^{n_{\alpha-1}-n_{\alpha-2}+r_{\alpha-2}-r_{\alpha-1}}\right) q^{n_\alpha-n_{\alpha-1}+r_{\alpha-1}-i}$$

$$= -\lambda'_{\alpha-1} q^{n_\alpha-n_{\alpha-1}+r_{\alpha-1}-i} + \lambda'''_\alpha q^{n_\alpha-n_{\alpha-2}+r_{\alpha-2}-i} = \ldots =$$

$$= -\sum_{k=1}^{\alpha-\gamma-1} \lambda'_{\alpha-k} q^{n_\alpha-n_{\alpha-k}+r_{\alpha-k}-i} + \lambda_\alpha^{(\alpha-\gamma+1)} q^{n_\alpha-n_\gamma+r_\gamma-i}$$

$$= -\sum_{k=1}^{\alpha-\gamma-1} \lambda'_{\alpha-k} q^{n_\alpha-n_{\alpha-k}+r_{\alpha-k}-i} + \left(-\lambda'_\gamma+\lambda_\alpha^{(\alpha-\gamma+2)} q^{i-m+n_\gamma-r_\gamma}\right) q^{n_\alpha-n_\gamma+r_\gamma-i}$$

$$= -\sum_{j=\gamma}^{\alpha-1} \lambda'_j q^{n_\alpha-n_j+r_j-i} + \lambda_\alpha^{(\alpha-\gamma+2)} q^{n_\alpha-m} .$$

Suppressing the superscripts, we have the required result. Converse is easy. //

In the rest of this section we will use the following system of notations, possibly with subscripts or superscripts. The meaning of symbols different from those below will be clear from the context.

Elements of U : $\bar{x}, \bar{y}$.

Elements of $\langle \bar{a}_i, \bar{b}_i : i = 1, \ldots, \alpha \rangle$: $\bar{u}, \bar{v}$.

Elements of $\langle \bar{a}_{jk}, \bar{b}_{jk} : k = 1, \ldots, \varepsilon_j , \ 1 \le j \le l \rangle$: $\bar{c}, \bar{d}$.

Isometries of U : $\bar{\varphi}, \bar{\psi}$.

Elements of Z_{q^m} : $\lambda, \mu, \nu, \rho, \sigma, \tau$.

Recall the definition of $QSp(\delta_1, \ldots, \delta_h)$. Though this was defined with $\delta_h > 0$, it will be convenient to adopt the convention that $QSp(\delta_1, \ldots, \delta_k, 0) = QSp(\delta_1, \ldots, \delta_k)$. The following lemmas show that we are justified in doing so and that $QSp(\delta_1, \ldots, \delta_h)$ and $QSp(U^t)$ arise naturally from $QSp(U)$.

4.2.18 LEMMA. *Let* $1 \le h \le l$, $\delta_h > 0$, $0 \le \delta_j \le \varepsilon_j$, $j = 1, \ldots, h$. *Then*

$QSp(\delta_1, \ldots, \delta_h) \cong \{\bar{\varphi} \in QSp(U) : \bar{a}_{jk}\bar{\varphi} = \bar{a}_{jk}$, $\bar{b}_{jk}\bar{\varphi} = b_{jk}$,

for $k = 1, \ldots, \varepsilon_j$, $h < j \le l$ *and* $k = \delta_j+1, \ldots, \varepsilon_j$, $1 \le j \le h\}$.

Proof. Let $\bar{\varphi} \in QSp(V)$ where $V = U(\delta_1, \ldots, \delta_h)$. We can extend $\bar{\varphi}$ to an element of $QSp(U)$ in the obvious way by letting $\bar{\varphi}$ act trivially on those generators $\bar{a}_{jk}, \bar{b}_{jk}$ of U which are not in V . On the other hand, suppose $\bar{\varphi} \in QSp(U)$ where

$$\bar{a}_i\bar{\varphi} = \bar{u}_i + \bar{c}_i , \quad \bar{b}_i\bar{\varphi} = \bar{v}_i + \bar{d}_i , \quad i = 1, \ldots, \alpha ,$$

$$\bar{a}_{jk}\bar{\varphi} = \bar{u}_{jk} + \bar{c}_{jk} , \quad \bar{b}_{jk}\bar{\varphi} = \bar{v}_{jk} + \bar{d}_{jk} , \quad k = 1, \ldots, \varepsilon_j , \ 1 \le j \le l .$$

Let W be the submodule of U generated by those generators $\bar{a}_{jk}, \bar{b}_{jk}$ which are not in V . If $\bar{\varphi}$ is trivial on these generators, it is clear that $\bar{c}_i, \bar{d}_i, \bar{c}_{jk}, \bar{d}_{jk} \in W^{\perp}$ for all $i = 1, \ldots, \alpha$, $k = 1, \ldots, \varepsilon_j$, $1 \le j \le h$, and hence $\bar{a}_i\bar{\varphi}, \bar{b}_i\bar{\varphi}, \bar{a}_{jk}\bar{\varphi}, \bar{b}_{jk}\bar{\varphi} \in V$ for all $i = 1, \ldots, \alpha$, $k = 1, \ldots, \delta_j$, $1 \le j \le h$. In other words, $\varphi|_V \in Sp(V)$. Consequently the restriction mapping on those elements of $QSp(U)$ which fix the generators $\bar{a}_{jk}, \bar{b}_{jk}$ not in V , gives the required isomorphism. //

4.2.19 LEMMA. *Let* $\bar{a} = \bar{a}_{h\delta_h}$, $\bar{b} = \bar{b}_{h\delta_h}$, $\delta_h > 1$. *Then*

$$\{\bar{\varphi} \in QSp(\delta_1, \ldots, \delta_h) : \bar{a}\bar{\varphi} = \bar{a}\ ,\ \bar{b}\bar{\varphi} = \bar{b}\} \cong QSp(\delta_1, \ldots, \delta_{h-1}, \delta_h{-}1)\ .$$

Proof. As in the proof of Lemma 4.2.18, the group of isometries on the left is isomorphic to the group of isometries of U which fix all those generators $\bar{a}_{jk}, \bar{b}_{jk}$ not in $U(\delta_1, \ldots, \delta_{h-1}, \delta_h{-}1)$, and hence by Lemma 4.2.18, is isomorphic to $QSp(\delta_1, \ldots, \delta_{h-1}, \delta_h{-}1)$. //

In particular with $\delta_h = 1$, a similar argument shows that

4.2.20 LEMMA.

$$\{\bar{\varphi} \in QSp(\delta_1, \ldots, \delta_{h-1}, 1) : \bar{a}_{h1}\bar{\varphi} = \bar{a}_{h1}\ ,\ \bar{b}_{h1}\bar{\varphi} = \bar{b}_{h1}\} \cong QSp(\delta_1, \ldots, \delta_{h-1})\ .$$

We have analogues of the above lemmas for $QSp(U^t)$. Since the proofs are similar to those above, we omit them.

4.2.21 LEMMA. $\{\bar{\varphi} \in QSp(1) : \bar{a}_{11}\bar{\varphi} = \bar{a}_{11}\ ,\ \bar{b}_{11}\bar{\varphi} = \bar{b}_{11}\} \cong QSp(U^1)$.

4.2.22 LEMMA. *Let* $1 \le t \le \alpha$. *Then* $QSp(U^t)$ *is isomorphic to the group of elements of* $QSp(U)$ *which act trivially on the generators* $\bar{a}_i, \bar{b}_i, \bar{a}_{jk}, \bar{b}_{jk}$ *for* $i = 1, \ldots, t{-}1$, $k = 1, \ldots, \varepsilon_j$, $1 \le j \le l$.

4.2.23 LEMMA. *Let* $1 \le t < \alpha$. *Then*

$$\left\{\bar{\varphi} \in QSp(U^t) : \bar{a}_t\bar{\varphi} = \bar{a}_t\ ,\ \bar{b}_t\bar{\varphi} = b_t\right\} \cong QSp(U^{t+1})\ .$$

Associated with each $U(\delta_1, \ldots, \delta_h)$ we define the following submodule

$$W(\delta_1, \ldots, \delta_h) = \langle \bar{a}_{jk}, \bar{b}_{jk} : k = 1, \ldots, \delta_j\ ,\ 1 \le j \le h\rangle\ .$$

For the moment denote this submodule by W. By Lemma 4.2.9, $(\bar{a}_{jk}, \bar{b}_{jk}) = q^{m-j}$, $1 \le j \le l$. Hence $q^h\bar{c} = 0$ for all $\bar{c} \in W$ so that W is a Z_{q^h}-module. Moreover $q^h(\bar{c}, \bar{d}) = (q^h\bar{c}, \bar{d}) = 0$ and so $(\bar{c}, \bar{d}) \equiv 0 \pmod{q^{m-h}}$ for all $\bar{c}, \bar{d} \in W$. We will denote W when considered as such a Z_{q^h}-module by $W^*(\delta_1, \ldots, \delta_h)$ or simply W^*.

We can then define a Z_{q^h}-bilinear form on W^* as follows

$$(\cdot, \cdot)_* : W^* \times W^* \to Z_{q^h} ,$$

$$(\bar{c}, \bar{d})_* = q^{-(m-h)}(\bar{c}, \bar{d}) .$$

It is easily checked that $(\cdot, \cdot)_*$ is a non-degenerate alternating form on W^* so that W^* is a non-degenerate symplectic module over Z_{q^h}. It is, in fact, canonic since $(a_{h1}, b_{h1})_* = 1$. W^* has a symplectic decomposition

$$W^* = W_1^* \perp \ldots \perp W_h^* ,$$

where $W_{h-j+1}^* = \langle \bar{a}_{j1}, \bar{b}_{j1} \rangle \perp \ldots \perp \langle \bar{a}_{j\delta_j}, \bar{b}_{j\delta_j} \rangle$, $j = 1, \ldots, h$,

and $(\bar{a}_{jk}, \bar{b}_{jk})_* = q^{h-j}$, $k = 1, \ldots, \delta_j$, $1 \le j \le h$. The symplectic sequence of W^* is $[\delta_h, \ldots, \delta_1]$.

Recall that an invertible pair of W^* is an ordered pair $[\bar{c}, \bar{d}]$ of elements of W^* such that $(\bar{c}, \bar{d})_*$ is invertible. We now show that the qhp's of $U(\delta_1, \ldots, \delta_h)$ are related to the invertible pairs of W^* . This will be of significance in the proof of Lemma 4.2.25.

4.2.24 LEMMA. *Let* $[\bar{x}, \bar{y}]$ *be a qhp of* $U(\delta_1, \ldots, \delta_h)$ *and let* $\bar{x} = \bar{u} + \bar{c}$, $\bar{y} = \bar{v} + \bar{d}$. *Then* $[\bar{c}, \bar{d}]$ *is an invertible pair of* $W^*(\delta_1, \ldots, \delta_h)$.

Proof. It is enough to show that $(\bar{u}, \bar{v}) \equiv 0 \pmod{q^{m-h+1}}$. For we would then have $q^{m-h} = (\bar{x}, \bar{y}) = (\bar{u}, \bar{v}) + (\bar{c}, \bar{d}) = \lambda q^{m-h+1} + (\bar{c}, \bar{d})$ and so $(\bar{c}, \bar{d})_* = 1 - \lambda q$ is invertible. By definition, $x, y \in D_h$ and hence are given explicitly by Lemmas 4.2.13-4.2.17. We consider two cases.

Case 1. $h \in I_\beta$, $0 \le \beta \le \alpha$. Then Lemmas 4.2.13, 4.2.15 and 4.2.16 tell us that $\bar{u}$, $\bar{v}$ are of the forms

$$\bar{u} = \sum_{j=1}^{\beta} (\lambda_j \bar{a}_j + \mu_j \bar{b}_j) q^{r_j - h} + \sum_{j=\beta+1}^{\alpha} \left\{ \left(-\lambda_{j-1}^* + \lambda_j^* q^{n_j - n_{j+1}} \right) \bar{a}_j + \mu_j \bar{b}_j \right\} ,$$

$$\bar{v} = \sum_{j=1}^{\beta} (\rho_j \bar{a}_j + \sigma_j \bar{b}_j) q^{r_j - h} + \sum_{j=\beta+1}^{\alpha} \left\{ \left(-\rho_{j-1}^* + \rho_j^* q^{n_j - n_{j+1}} \right) \bar{a}_j + \sigma_j \bar{b}_j \right\} ,$$

where $\lambda_\beta^* = \sum_{j=1}^{\beta} \lambda_j q^{n_{\beta+1}-n_j+r_j-h}$, $\rho_\beta^* = \sum_{j=1}^{\beta} \rho_j q^{n_{\beta+1}-n_j+r_j-h}$. Hence

$$(\bar{u}, \bar{v}) = \sum_{j=1}^{\beta} (\lambda_j\sigma_j - \mu_j\rho_j) q^{m-h+r_j-h}$$

$$+ \sum_{j=\beta+1}^{\alpha} \left\{ (\mu_j\rho_{j-1}^* - \sigma_j\lambda_{j-1}^*) + (\sigma_j\lambda_j^* - \mu_j\rho_j^*) q^{n_j-n_{j+1}} \right\} q^{m-r_j} .$$

The first sum $\equiv 0 \pmod{q^{m-h+1}}$ since $r_j > h$ for $j = 1, \ldots, \beta$.

The second sum $\equiv 0 \pmod{q^{m-h+1}}$ because if $h > r_{\beta+1}$, then $m-r_j > m-h$ for $j = \beta+1, \ldots, \alpha$, while if $h = r_{\beta+1}$, then $m-r_j > m-h$ for $j = \beta+2, \ldots, \alpha$, and q divides λ_β^* , ρ_β^* . Therefore

$$(\bar{u}, \bar{v}) \equiv 0 \pmod{q^{m-h+1}}.$$

Case 2. $h \in I_\beta$, $1 \le \beta \le \alpha$. By Lemma 4.2.14 and 4.2.17, $\bar{u}, \bar{v}$ are of the forms

$$\bar{u} = \sum_{j=1}^{\beta-1} (\lambda_j\bar{a}_j + \mu_j\bar{b}_j) q^{r_j-h} + (-\lambda^* + \lambda_\beta q^{n_\beta - n_{\beta+1}})\bar{a}_\beta + \mu_\beta q^{r_\beta - h}\bar{b}_\beta +$$

$$+ \sum_{j=\beta+1}^{\alpha} \left\{ \left(-\lambda_{j-1} + \lambda_j q^{n_j-n_{j+1}} \right)\bar{a}_j + \mu_j\bar{b}_j \right\} ,$$

$$\bar{v} = \sum_{j=1}^{\beta-1} (\rho_j\bar{a}_j + \sigma_j\bar{b}_j) q^{r_j-h} + \left(-\rho^* + \rho_\beta q^{n_\beta - n_{\beta+1}} \right)\bar{a}_\beta + \sigma_\beta q^{r_\beta - h}\bar{b}_\beta$$

$$+ \sum_{j=\beta+1}^{\alpha} \left\{ \left(-\rho_{j-1} + \rho_j q^{n_j-n_{j+1}} \right)\bar{a}_j + \sigma_j\bar{b}_j \right\} .$$

where $\lambda^* = \sum_{j=1}^{\beta-1} \lambda_j q^{n_\beta - n_j + r_j - h}$, $\rho^* = \sum_{j=1}^{\beta-1} \rho_j q^{n_\beta - n_j + r_j - h}$. Hence

$$(\bar{u}, \bar{v}) = \sum_{j=1}^{\beta-1} (\lambda_j\sigma_j - \mu_j\rho_j) q^{m-h+r_j-h}$$

$$+ \left\{ (\mu_\beta\rho^* - \sigma_\beta\lambda^*) + (\lambda_\beta\sigma_\beta - \mu_\beta\rho_\beta) q^{n_\beta - n_{\beta+1}} \right\} q^{m-h} + \sum_{j=\beta+1}^{\alpha} \xi_j q^{m-r_j} ,$$

where ξ_j is some complicated expression whose exact form need not bother us. The first sum $\equiv 0 \pmod{q^{m-h+1}}$ since $r_j > h$ for

$j = 1, \ldots, \beta-1$. The second term $\equiv 0 \pmod{q^{m-h+1}}$ since

$$n_\beta - n_1 + r_1 - h > \ldots > n_\beta - n_{\beta-1} + r_{\beta-1} - h > n_\beta - n_\beta + r_\beta - h > 0$$

implies that q divides λ^*, ρ^* . Finally the last sum $\equiv 0 \pmod{q^{m-h+1}}$ because $m - r_j > m-h$ for $j = \beta+1, \ldots, \alpha$. Hence the assertion on $(\bar{u}, \bar{v})$ is proved. //

We can now prove the following useful lemma.

4.2.25 LEMMA. *Suppose G has the canonic decomposition*

$$G \tilde{=} Q(n_1, r_1) \ldots Q(n_\alpha, r_\alpha) Q(h) , \quad r_\alpha \geq 0 .$$

Let $x, y \in G$ such that $\langle x, y \rangle \tilde{=} Q(h)$. Then there exists $M \leq G$ such that $M \tilde{=} Q(n_1, r_1) \ldots Q(n_\alpha, r_\alpha)$, and $G = M\langle x, y \rangle$ is a central product of M and $\langle x, y \rangle$.

Proof. Case 1. $h \geq r_1$. Then $G' = \langle [x, y] \rangle$. As in the proof of 2.1, Brady, Bryce and Cossey [4], there exists $M \leq G$ such that $G = M\langle x, y \rangle$ is a central product of M and $\langle x, y \rangle$. Thus M has cyclic centre. The canonic decomposition of M cannot contain any $Q(j)$; otherwise, by Corollary 2.2.7, the canonic decomposition of G would contain more than one $Q(j)$, which is not so. Hence M has the canonic decomposition

$$M \tilde{=} Q(n_1', r_1') \ldots Q(n_\beta', r_\beta') .$$

If $r_\beta' = 0$ and $n_\beta' \leq h$, then $Q(n_\beta', 0)Q(h) = Q(h)$ by Lemma 2.2.3. If $r_\beta' > 0$ and $n_\beta' \leq h$, then $Q(n_\beta', r_\beta')Q(h) = Q(r_\beta')Q(h)$ by Lemma 2.2.5 and so the canonic decomposition of G contains more than one $Q(j)$, which is a contradiction. Hence $n_\beta' > h$. In other words, G has the canonic decomposition

$$G \tilde{=} Q(n_1', r_1') \ldots Q(n_\beta', r_\beta')Q(h) .$$

By Theorem 2.3.16, $\beta = \alpha$, $n_i' = n_i$, $r_i' = r_i$, $i = 1, \ldots, \alpha$.

Case 2. $h < r_1$. First we produce elements $x_1, y_1 \in G$ such that $\langle x_1, y_1 \rangle$ centralizes $\langle x, y \rangle$, and $\langle x_1, y_1 \rangle \tilde{=} Q(n_1, r_1)$. To do this, we work within the module $U = U(0, \ldots, 0, 1)$ (with $h-1$ zeros) associated with G . Clearly we may suppose $[\bar{x}, \bar{y}]$ is a qhp of U . Let

$$\bar{x} = \bar{u} + \bar{c} \ , \quad \bar{y} = \bar{v} + \bar{d} \ ,$$

where $\bar{c}, \bar{d} \in W^* = W^*(0, \ldots, 0, 1)$. Then by Lemma 4.2.24, $[\bar{c}, \bar{d}]$ is an invertible pair of W^* , and hence $W^* = \langle \bar{c}, \bar{d} \rangle$. We may assume $(\bar{c}, \bar{d})_* = 1$. Since $q^h\bar{u} = q^h\bar{v} = 0$, it follows that

$$(\bar{a}_1, \bar{u}) = \lambda q^{m-h} \ , \quad (\bar{a}_1, \bar{v}) = \mu q^{m-h} \ ,$$

$$(\bar{b}_1, \bar{u}) = \rho q^{m-h} \ , \quad (\bar{b}_1, \bar{v}) = \sigma q^{m-h} \ .$$

Put $\bar{x}_1 = \bar{a}_1 + \bar{c}_1$, $\bar{y}_1 = \tau\bar{b}_1 + \bar{d}_1$, where

$$\bar{c}_1 = -\mu\bar{c} + \lambda\bar{d} \ , \quad \bar{d}_1 = \tau(-\sigma\bar{c}+\rho\bar{d}) \ ,$$

$$\tau = \left\{1+(\lambda\sigma-\mu\rho)q^{r_1-h}\right\}^{-1} \ .$$

It is easily verified that $(\bar{x}_1, \bar{y}_1) = (\bar{a}_1, \bar{b}_1)$, $\langle \bar{x}_1, \bar{y}_1 \rangle \perp \langle \bar{x}, \bar{y} \rangle$. Hence $\langle x_1, y_1 \rangle$ centralizes $\langle x, y \rangle$, and $G' = \langle [x_1, y_1] \rangle$. As in Case 1, $G = \langle x_1, y_1 \rangle H$ is a central product of $\langle x_1, y_1 \rangle$ and $H \leq G$. Thus $\langle x_1, y_1 \rangle$ has cyclic centre, and since $|x_1| = q^{n_1}$, we have $\langle x_1, y_1 \rangle \cong Q(n_1, r_1)$.

We use induction on the exponent of G to complete the proof. Write $N = \langle x_1, y_1 \rangle$. Then $C_G(N) = Z(N)H$. First suppose $Z(N) \leq Z(H)$, so that $C_G(N) = H$ and $x, y \in H$. Again the canonic decomposition of H cannot contain more than one $Q(j)$. Suppose the canonic decomposition of H contains no $Q(j)$ at all, say

$$H \cong Q(n'_2, r'_2) \ldots Q(n'_\beta, r'_\beta) \ ,$$

with $n_1 \geq n'_2$, $r_1 \geq r'_2$. If $n_1 = n'_2$, then by Lemmas 2.2.1 and 2.2.4, $\langle x_1, y_1 \rangle Q(n'_2, r'_2) \cong Q(n'_2, r'_2)Q(r_1)$, so that $Q(r_1)$ occurs in the canonic decomposition of G , which is not so. Hence $n_1 > n'_2$. If $r_1 = r'_2$, we get a similar contradiction, and hence $r_1 > r'_2$. If $r'_2 = 0$, H is cyclic, contradicting $x, y \in H$. Hence $r'_2 > 0$. If $n_1-r_1 \geq n'_2-r'_2$, then by Lemma 2.2.2,

$\langle x_1, y_1\rangle Q(n_2', r_2') \cong Q(n_1, r_1)Q(r_2')$, and so $r_2' = h$, which means $H' = \langle [x, y] \rangle$. By the usual procedure, H would then contain $Q(h)$ in its canonic decomposition, which is a contradiction. Hence $n_1 - r_1 < n_2' - r_2'$. This means that the canonic decomposition of G is

$$G \cong Q(n_1, r_1)Q(n_2', r_2') \ldots Q(n_\beta', r_\beta') ,$$

which is again a contradiction. Hence the canonic decomposition of H contains precisely one $Q(j)$, namely $Q(h)$. By a similar argument, we conclude that

$$H \cong Q(n_2, r_2) \ldots Q(n_\alpha, r_\alpha)Q(h) .$$

So by the induction hypothesis, there exists $M_1 \leq H$ such that $M_1 \cong Q(n_2, r_2) \ldots Q(n_\alpha, r_\alpha)$, and $H = M_1\langle x, y\rangle$ is a central product of M_1 and $\langle x, y\rangle$. Put $M = NM_1$.

Finally suppose $Z(N) > Z(H)$. Write $Z(N) = Q(r, 0)$. By an argument similar to that used above, we can show that the canonic decomposition of $Z(N)H$ is

$$Z(N)H \cong Q(n_2, r_2) \ldots Q(n_\alpha, r_\alpha)Q(r, 0)Q(h) .$$

Since $x, y \in Z(N)H$ and $n_2 < n_1$, we can use induction as we did before. //

The following lemma will also be useful.

4.2.26 LEMMA. *Suppose G has the canonic decomposition*

$$G \cong Q(n_1, r_1) \ldots Q(n_\alpha, r_\alpha) , \quad r_\alpha \geq 0 .$$

Let $x, y \in G$ such that $\langle x, y\rangle \cong Q(n_1, r_1)$. Then there exists $M \leq G$ such that $M \cong Q(n_2, r_2) \ldots Q(n_\alpha, r_\alpha)$, and $G = \langle x, y\rangle M$ is a central product of $\langle x, y\rangle$ and M .

Proof. Since $G' = \langle [x, y]\rangle$, we can use the usual procedure to produce $M \leq G$ such that $G = \langle x, y\rangle M$ is a central product of $\langle x, y\rangle$ and M . The canonic decomposition of M cannot contain any $Q(j)$ and so must be of the form

$$M \cong Q(n_2', r_2') \ldots Q(n_\beta', r_\beta')$$

with $n_1 \geq n_2'$, $r_1 \geq r_2'$. By an argument similar to that used in

Case 2 of the proof of Lemma 4.2.25, we conclude that $n_1 > n_2'$, $r_1 > r_2'$ and $n_1 - r_1 < n_2' - r_2'$. Thus

$$G \cong Q(n_1, r_1)Q(n_2', r_2') \ldots Q(n_\beta', r_\beta')$$

is the canonic decomposition of G. Hence by Theorem 2.3.16, $\beta = \alpha$, $n_i' = n_i$, $r_i' = r_i$, $i = 2, \ldots, \alpha$. //

We can now shed some light on the relationship between $QSp(\delta_1, \ldots, \delta_h)$ and the qhp's of $U(\delta_1, \ldots, \delta_h)$.

4.2.27 LEMMA. *Let $[\bar{x}, \bar{y}]$ be a qhp of $U(\delta_1, \ldots, \delta_h)$. Then there exists $\bar{\varphi} \in QSp(\delta_1, \ldots, \delta_h)$ such that $\bar{a}_{h1}\bar{\varphi} = \bar{x}$, $\bar{b}_{h1}\bar{\varphi} = \bar{y}$.*

Proof. Let $\bar{x} = \bar{u} + \bar{c}$, $\bar{y} = \bar{v} + \bar{d}$. Then $[\bar{c}, \bar{d}]$ is an invertible pair of $W^* = W^*(\delta_1, \ldots, \delta_h)$. We may assume that $[\bar{c}, \bar{d}]$ is a hyperbolic pair of W^*. Then by Lemma 4.1.11, W^* has a symplectic decomposition $W^* = W_1^* \perp \ldots \perp W_h^*$, where $W_j^* = \langle \bar{c}_{j1}, \bar{d}_{j1} \rangle \perp \ldots \perp \langle \bar{c}_{j\delta_j}, \bar{d}_{j\delta_j} \rangle$, $j = 1, \ldots, h$, and $(\bar{c}_{jk}, \bar{d}_{jk}) = q^{j-1}$ with $\bar{c}_{11} = \bar{c}$, $\bar{d}_{11} = \bar{d}$.

Put $H = \langle a_1, b_1, \ldots, a_\alpha, b_\alpha, c, d \rangle$, and N to be the subgroup generated by all the other c_{jk}, d_{jk} together with those a_{jk}, b_{jk} for which $\bar{a}_{jk}, \bar{b}_{jk}$ are not in W^*. It is then clear that $G = HN$ is the central product of H and N. But H itself is the central product with cyclic centre of $\langle a_1, b_1, \ldots, a_\alpha, b_\alpha \rangle$ and $\langle c, d \rangle$. Thus $\langle c, d \rangle$ has cyclic centre, and since c and $[c, d]$ both have orders q^h, $\langle c, d \rangle \cong Q(h)$. Hence

$$H \cong Q(n_1, r_1) \ldots Q(n_\alpha, r_\alpha)Q(h).$$

Since $[\bar{x}, \bar{y}]$ is a qhp, $x, y \in D_h$ and hence $x, y, [x, y]$ have orders q^h. Clearly then we may suppose $x, y \in H$. Moreover $\langle x, y \rangle$ has cyclic centre and so $\langle x, y \rangle \cong Q(h)$. By Lemma 4.2.25, there exists $M \leq H$ such that $M \cong Q(n_1, r_1) \ldots Q(n_\alpha, r_\alpha)$ and $H = M\langle x, y \rangle$ is the central product of M and $\langle x, y \rangle$. Let x_i, y_i,

$i = 1, \ldots, \alpha$, be canonic generators of M so that $x_i \in A_i$, $y_i \in B_i$. Plainly the following mapping $\bar{\varphi}$ defines an element of $QSp(\delta_1, \ldots, \delta_h)$ satisfying the lemma:

$$\bar{a}_i\bar{\varphi} = \bar{x}_i \ , \quad \bar{b}_i\bar{\varphi} = \bar{y}_i \ , \quad i = 1, \ldots, \alpha \ ,$$

$$\bar{a}_{h1}\bar{\varphi} = \bar{x} \ , \quad \bar{b}_{h1}\bar{\varphi} = \bar{y} \ ,$$

$$\bar{a}_{jk}\bar{\varphi} = \bar{c}_{jk} \ , \ \bar{b}_{jk}\bar{\varphi} = \bar{d}_{jk} \quad \text{for} \quad 1 < k \leq \delta_h \quad \text{if} \quad j = h \ ,$$

and $k = 1, \ldots, \delta_j$ if $1 \leq j < h$. //

We have the following analogue for the qhp's of U^t .

4.2.28 LEMMA. *Let* $[\bar{x}, \bar{y}]$ *be a qhp of* U^t . *Then there exists* $\bar{\varphi} \in QSp(U^t)$ *such that* $\bar{a}_t\bar{\varphi} = \bar{x}$, $\bar{b}_t\bar{\varphi} = \bar{y}$.

Proof. We may suppose $x, y \in H = \langle a_t, b_t, \ldots, a_\alpha, b_\alpha \rangle$. By definition $[x, y]$ has order q^{r_t} and hence $H' = \langle [x, y] \rangle$. As in the proof of 2.2, Brady, Bryce and Cossey [4], $H = \langle x, y \rangle H_1$ is a central product of $\langle x, y \rangle$ and some $H_1 \leq H$. So $\langle x, y \rangle$ has cyclic centre and since x has order q^{n_t} , $\langle x, y \rangle \tilde{=} Q(n_t, r_t)$. Finally by Lemma 4.2.26, $H = \langle x, y \rangle M$ is a central product of $\langle x, y \rangle$ and M , where $M \tilde{=} Q(n_{t+1}, r_{t+1}) \ldots Q(n_\alpha, r_\alpha)$. It is then evident that we can define $\bar{\varphi} \in QSp(U^t)$ such that $\bar{a}_t\bar{\varphi} = \bar{x}$. $\bar{b}_t\bar{\varphi} = \bar{y}$. //

The usefulness of Lemmas 4.2.27 and 4.2.28 lies in their application to prove Lemmas 4.2.3 and 4.2.4. We have gone a long way to set up the machinery to prove Lemma 4.2.5 which shows that we only have to calculate $\tilde{\omega}(\varepsilon_1, \ldots, \varepsilon_{i-1}, j)$ and $\tilde{\omega}_t$, that is, the numbers of qhp's of $U(\varepsilon_1, \ldots, \varepsilon_{i-1}, j)$ and U^t . First we calculate $\tilde{\omega}(\varepsilon_1, \ldots, \varepsilon_{i-1}, j)$ in terms of $\omega(\varepsilon_1, \ldots, \varepsilon_{i-1}, j)$, the number of hyperbolic pairs of the canonic non-degenerate symplectic module $W^*(\varepsilon_1, \ldots, \varepsilon_{i-1}, j)$ over Z_{q^i} . The latter quantity is given by Lemma 4.1.16. Lastly the calculation of $\tilde{\omega}_t$ is more straightforward.

4.2.29 LEMMA. *Let* $i \in I_\beta$, $0 \le \beta \le \alpha$. *Then*

$$\log_q \tilde{\omega}(\varepsilon_1, \ldots, \varepsilon_{i-1}, j) = 4 \sum_{k=\beta+1}^{\alpha} r_k + 4\beta i + 2(m-n_{\beta+1}) + \log_q \omega(\varepsilon_1, \ldots, \varepsilon_{i-1}, j) .$$

Proof. Let $\bar{x}, \bar{y} \in V = U(\varepsilon_1, \ldots, \varepsilon_{i-1}, j)$ where $x, y \in D_i$ and $\bar{x} = \bar{u} + \bar{c}$, $\bar{y} = \bar{v} + \bar{d}$. As in the proof of Lemma 4.2.24, $(\bar{u}, \bar{v}) = \lambda q^{m-i+1}$. Put $\mu = 1 - \lambda q$. Note that μ is uniquely determined modulo q^i by $\bar{u}, \bar{v}$. Call $[\bar{c}, \bar{d}]$ a μ-pair of $W^* = W^*(\varepsilon_1, \ldots, \varepsilon_{i-1}, j)$ if $(\bar{c}, \bar{d})_* = \mu$, where we keep $\bar{u}, \bar{v}$ fixed for the moment.

We claim that $[\bar{x}, \bar{y}]$ is a qhp of V if and only if $[\bar{c}, \bar{d}]$ is a μ-pair of W^* . First, if $[\bar{x}, \bar{y}]$ is a qhp, then $(\bar{x}, \bar{y}) = q^{m-i}$ and so $q^{m-i} = \lambda q^{m-i+1} + (\bar{c}, \bar{d})$, or $(\bar{c}, \bar{d})_* = 1 - \lambda q = \mu$. Conversely, if $[\bar{c}, \bar{d}]$ is a μ-pair of W^* , then

$$(\bar{x}, \bar{y}) = (\bar{u}, \bar{v}) + (\bar{c}, \bar{d}) = \lambda q^{m-i+1} + \mu q^{m-i} = q^{m-i} ,$$

and so $[\bar{x}, \bar{y}]$ is a qhp.

For a fixed invertible μ , the number of μ-pairs of W^* is precisely $\omega(W^*)$, the number of hyperbolic pairs of W^* , as can be seen from the one-to-one correspondence $[\bar{c}, \bar{d}] \mapsto [\mu^{-1}\bar{c}, \bar{d}]$ from the μ-pairs onto the hyperbolic pairs of W^* . Consequently for each fixed pair $[\bar{u}, \bar{v}]$ of elements of V of the appropriate forms, there are $\omega(W^*)$ pairs $[\bar{c}, \bar{d}]$ of elements of W^* such that $[\bar{x}, \bar{y}]$ is a qhp of V . So it only remains to enumerate the distinct pairs $[\bar{u}, \bar{v}]$. Each of the $\bar{u}, \bar{v}$ is given in Case 1 of the proof of Lemma 4.2.24 by replacing h by i . Hence we have the following freedom of choice:

each $\lambda_k, \mu_k, \rho_k, \sigma_k$, $k = 1, \ldots, \beta$, can take q^i values,

each μ_k, σ_k , $k = \beta+1, \ldots, \alpha$, can take q^{r_k} values,

each λ_k^*, ρ_k^* , $k = \beta+1, \ldots, \alpha$, can take $q^{r_k - n_k + n_{k+1}}$ values.

An easy enumeration then gives the required expression for $\tilde{\omega}(\varepsilon_1, \ldots, \varepsilon_{i-1}, j)$. //

4.2.30 LEMMA. *Let* $i \in J_\beta$, $1 \le \beta \le \alpha$. *Then*

$$\log_q \tilde{\omega}(\varepsilon_1, \ldots, \varepsilon_{i-1}, j) = 4 \sum_{k=\beta+1}^{\alpha} r_k + 2i(\beta-1) + 2(m-n_\beta+r_\beta) + \log_q \omega(\varepsilon_1, \ldots, \varepsilon_{i-1}, j) .$$

Proof. Since the proof is similar to that of Lemma 4.2.29, we omit the details. Suffice it to say that we only have to enumerate the distinct pairs $[\bar{u}, \bar{v}]$ where $\bar{u}, \bar{v}$ are given in Case 2 of the proof of Lemma 4.2.24 with h replaced by i . We then have the following freedom of choice:

each $\mu_\beta, \sigma_\beta, \lambda_k, \mu_k, \rho_k, \sigma_k$, $k = 1, \ldots, \beta-1$, can take q^i values,

each λ_k, ρ_k , $k = \beta, \ldots, \alpha$, can take $q^{r_k - n_k + n_{k+1}}$ values,

each μ_k, σ_k , $k = \beta+1, \ldots, \alpha$, can take q^{r_k} values.

An easy enumeration gives the required result. //

4.2.31 LEMMA. *With* s_i, t_i , $i = 1, \ldots, l$, *defined in the set of notations preceding Theorem* 4.2.6,

$$\sum_{i=1}^{l} \sum_{j=1}^{\varepsilon_i} \log_q \tilde{\omega}(\varepsilon_1, \ldots, \varepsilon_{i-1}, j) = 2 \sum_{i=1}^{l} (s_i + i t_i)\varepsilon_i + \sum_{i=1}^{l} \sum_{j=1}^{\varepsilon_i} \log_q \omega(\varepsilon_1, \ldots, \varepsilon_{i-1}, j) .$$

Proof. With reference to the remarks preceding Theorem 4.2.6, we have

$$\{1, 2, \ldots, l\} = I_0 \cup I_1 \cup \ldots \cup I_\alpha \cup J_1 \cup \ldots \cup J_\alpha ,$$

where the union is disjoint. Hence

$$\prod_{i=1}^{l}\prod_{j=1}^{\varepsilon_i}\tilde{\omega}(\varepsilon_1, \ldots, \varepsilon_{i-1}, j)$$

$$= \prod_{\beta=0}^{\alpha}\prod_{i\in I_\beta}\prod_{j=1}^{\varepsilon_i}\tilde{\omega}(\varepsilon_1, \ldots, \varepsilon_{i-1}, j) \cdot \prod_{\beta=1}^{\alpha}\prod_{i\in J_\beta}\prod_{j=1}^{\varepsilon_i}\tilde{\omega}(\varepsilon_1, \ldots, \varepsilon_{i-1}, j) .$$

By Lemma 4.2.29, the first factor is equal to

$$q^{\gamma_1}\prod_{\beta=0}^{\alpha}\prod_{i\in I_\beta}\prod_{j=1}^{\varepsilon_i}\omega(\varepsilon_1, \ldots, \varepsilon_{i-1}, j) ,$$

where

$$\gamma_1 = \sum_{\beta=0}^{\alpha}\sum_{i\in I_\beta}\sum_{j=1}^{\varepsilon_i}\left\{4\sum_{k=\beta+1}^{\alpha} r_k + 4\beta i + 2(m-n_{\beta+1})\right\}$$

$$= 2\sum_{\beta=0}^{\alpha}\sum_{i\in I_\beta}(s_i + it_i)\varepsilon_i ,$$

where $s_i = 2\sum_{k=\beta+1}^{\alpha} r_k + m - n_{\beta+1}$, $t_i = 2\beta$ for $i \in I_\beta$. By Lemma 4.2.30, the second factor is equal to

$$q^{\gamma_2}\prod_{\beta=1}^{\alpha}\prod_{i\in J_\beta}\prod_{j=1}^{\varepsilon_i}\omega(\varepsilon_1, \ldots, \varepsilon_{i-1}, j) ,$$

where

$$\gamma_2 = \sum_{\beta=1}^{\alpha}\sum_{i\in J_\beta}\sum_{j=1}^{\varepsilon_i}\left\{4\sum_{k=\beta+1}^{\alpha} r_k + 2i(2\beta-1) + 2(m-n_\beta+r_\beta)\right\}$$

$$= 2\sum_{\beta=1}^{\alpha}\sum_{i\in J_\beta}(s_i+it_i)\varepsilon_i ,$$

where $s_i = 2\sum_{k=\beta+1}^{\alpha} r_k + m - n_\beta + r_\beta$, $t_i = 2\beta - 1$ for $i \in J_\beta$.

Combining these results, we get the required expression. //

4.2.32 LEMMA. *Let* $0 \le t \le \alpha$. *Then*

$$\log_q \tilde{\omega}_t = 4 \sum_{k=t}^{\alpha} r_k + 2(m-n_t) - r_t .$$

Proof. Let $\bar{x}, \bar{y} \in U^t$ where $x \in A_t$, $y \in B_t$. Then by Lemmas 4.2.11 and 4.2.12, $\bar{x}, \bar{y}$ are of the forms

$$\bar{x} = \left(1+\lambda_t q^{n_t-n_{t+1}}\right)\bar{a}_t + \mu_t \bar{b}_t + \sum_{k=t+1}^{\beta} \left\{\left(-\lambda_{k-1}+\lambda_k q^{n_k-n_{k+1}}\right)\bar{a}_k+\mu_k\bar{b}_k\right\} ,$$

$$\bar{y} = \rho_t q^{n_t-n_{t+1}}\bar{a}_t + \sigma_t \bar{b}_t + \sum_{k=t+1}^{\alpha} \left\{\left(-\rho_{k-1}+\rho_k q^{n_k-n_{k+1}}\right)\bar{a}_k+\sigma_k\bar{b}_k\right\} .$$

Then $(\bar{x}, \bar{y}) = \left\{\sigma_t\left(1+\lambda_t q^{n_t-n_{t+1}}\right)-\mu_t\rho_t q^{n_t-n_{t+1}}\right\}q^{m-r_t} + \sum_{k=t+1}^{\alpha} \xi_k q^{m-r_k}$,

where ξ_k is some expression determined by $\lambda_k, \mu_k, \rho_k, \sigma_k$.

Now consider the following congruence (*) in the indeterminate σ,

$$\left(1+\lambda_t q^{n_t-n_{t+1}}\right)\sigma + \sum_{k=t+1}^{\alpha} \xi_k q^{r_t-r_k} \equiv 1 + \mu_t\rho_t q^{n_t-n_{t+1}} \pmod{q^{r_t}}.$$

It is then easily seen that $[\bar{x}, \bar{y}]$ is a qhp of U^t if and only if σ_t is a solution of (*). Moreover σ_t is uniquely determined modulo q^{r_t}. Hence we are allowed the following freedom of choice:

μ_t can take q^{r_t} values,

each λ_k, ρ_k, $k = t, \ldots, \alpha$, can take $q^{r_k-n_k+n_{k+1}}$ values,

each μ_k, σ_k, $k = t+1, \ldots, \alpha$, can take q^{r_k} values.

An easy calculation gives the required result. //

We have now completed the calculations.

4.3 Some extensions of certain results of D.L. Winter

Recall that a group G is a semi-direct product of A by B if $G = AB$, $A \lhd G$ and $A \cap B = 1$. We also say that G is a split

extension of A by B. We will continue to use the notations and terminology of the preceding two sections.

Winter [26] has proved that

(i) if $G = Q(1)^n$, then $\mathrm{aut}_Z G/\mathrm{inn}\, G \cong Sp(2n, q)$,

(ii) if $G = Q(2, 1)Q(1)^n$, then $\mathrm{aut}_Z G/\mathrm{inn}\, G$ is a semi-direct product of $Q(1)^n$ by $Sp(2n, q)$,

where $Sp(2n, q)$ is the symplectic group of dimension $2n$ over $\mathrm{GF}(q)$ (see Huppert [16]) for q odd. Using somewhat similar methods, we obtain the following extensions of his results.

4.3.1 THEOREM. *Let q be an odd prime.*

(i) If $G = Q(l)^{\varepsilon_l} \ldots Q(1)^{\varepsilon_1}$, $\varepsilon_l > 0$, then

$$\mathrm{aut}_Z G/\mathrm{inn}\, G \cong Sp(\varepsilon_1, \ldots, \varepsilon_l).$$

(ii) If $G = Q(n, r)Q(l)^{\varepsilon_l} \ldots Q(1)^{\varepsilon_1}$ where $n \geq 2r$, $n-r \geq l$, $\varepsilon_l > 0$, then $\mathrm{aut}_Z G/\mathrm{inn}\, G$ is a semi-direct product of H by $Sp(\varepsilon_1, \ldots, \varepsilon_l)$, where

$$H = \begin{cases} Q(r)^{\varepsilon_l + \ldots + \varepsilon_r} Q(r-1)^{\varepsilon_{r-1}} \ldots Q(1)^{\varepsilon_1} & \text{if } l \geq r, \\ Q(r, 0)Q(l)^{\varepsilon_l} \ldots Q(1)^{\varepsilon_1} & \text{if } l < r. \end{cases}$$

Proof of (i). By Theorem 4.2.2, $\mathrm{aut}_Z G/\mathrm{inn}\, G \cong QSp(U)$. But by the remarks following Theorem 4.2.6, $QSp(U) = Sp(U) = Sp(\varepsilon_1, \ldots, \varepsilon_l)$. //

The proof of *(ii)* is more involved. Let G be the group in Theorem 4.3.1 *(ii)* and let U be the corresponding module in 4.2. By virtue of Theorem 4.2.2, it is enough to show that $QSp(U)$ has the stated structure. We consider two cases: (a) $l \geq r$, (b) $l < r$.

The case when $l \geq r$. The relevant symbols related to $QSp(U)$ are $m = n - r$, $J_1 = \{i : 1 \leq i < r\}$, $I_0 = \{i : r \leq i \leq l\}$. We will write $a = a_1$, $b = b_1$. Using Lemmas 4.2.11, 4.2.12, 4.2.13 and

4.2.17, we can write down $QSp(U)$ explicitly. It is the group of isometries of U of the form

$$\left.\begin{aligned} \bar{a}\bar{\varphi} &= \bar{a} + \bar{b} + \bar{c} \\ \bar{b}\bar{\varphi} &= \bar{b} + \bar{d} \end{aligned}\right\}$$

$$\left.\begin{aligned} \bar{a}_{ij}\bar{\varphi} &= \mu_{ij}q^{r-i}\bar{b} + \bar{c}_{ij} \\ \bar{b}_{ij}\bar{\varphi} &= \sigma_{ij}q^{r-i}\bar{b} + \bar{d}_{ij} \end{aligned}\right\} j = 1, \ldots, \varepsilon_i , \quad 1 \le i < r ,$$

$$\left.\begin{aligned} \bar{a}_{ij}\bar{\varphi} &= \mu_{ij}\bar{b} + \bar{c}_{ij} \\ \bar{b}_{ij}\bar{\varphi} &= \sigma_{ij}\bar{b} + \bar{d}_{ij} \end{aligned}\right\} j = 1, \ldots, \varepsilon_i , \quad r \le i \le l .$$

Note that, in fact, $\bar{d} = 0$.

We now define two subgroups T_0, T_1 of $QSp(U)$. Let $T_0 = \{\bar{\varphi} \in QSp(U) : \bar{a}\bar{\varphi} = \bar{a} , \ \bar{b}\bar{\varphi} = \bar{b}\}$. It is clear that $T_0 \cong Sp(\varepsilon_1, \ldots, \varepsilon_l)$. Let T_1 be the set of isometries of U of the form

$$\left.\begin{aligned} \bar{a}\bar{\varphi} &= \bar{a} + \mu\bar{b} + \bar{c} \\ \bar{b}\bar{\varphi} &= \bar{b} \end{aligned}\right\}$$

$$\left.\begin{aligned} \bar{a}_{ij}\bar{\varphi} &= \mu_{ij}q^{r-i}\bar{b} + \bar{a}_{ij} \\ \bar{b}_{ij}\bar{\varphi} &= \sigma_{ij}q^{r-i}\bar{b} + \bar{b}_{ij} \end{aligned}\right\} j = 1, \ldots, \varepsilon_i , \quad 1 \le i < r ,$$

$$\left.\begin{aligned} \bar{a}_{ij}\bar{\varphi} &= \mu_{ij}\bar{b} + \bar{a}_{ij} \\ \bar{b}_{ij}\bar{\varphi} &= \sigma_{ij}\bar{b} + \bar{b}_{ij} \end{aligned}\right\} j = 1, \ldots, \varepsilon_i , \quad r \le i \le l .$$

Evidently, T_1 is a group. Note that $\bar{c}$ is uniquely determined by the values μ_{ij}, σ_{ij} . Theorem 4.3.1 *(ii)* for the case when $l \ge r$ then follows from the next six lemmas.

4.3.2 LEMMA. $QSp(U) = T_0T_1$, $T_0 \cap T_1 = 1$.

Proof. Plainly $T_0 \cap T_1 = 1$. Moreover

$$|T_0| = |Sp(\varepsilon_1, \ldots, \varepsilon_l)| ,$$

$$\log_q |T_1| = r + 2 \sum_{i=1}^{r-1} i\varepsilon_i + 2 \sum_{i=r}^{l} r\varepsilon_i .$$

Substituting the appropriate values into Theorem 4.2.6, we have

$$|QSp(U)| = |T_0| . |T_1| . \qquad //$$

4.3.3 LEMMA. $T_1 \triangleleft QSp(U)$.

Proof. It is enough to show that for every $\bar{\varphi}_i \in T_i$, $i = 0, 1$,

$$\bar{\varphi}_0 \bar{\varphi}_1 \bar{\varphi}_0^{-1} \in T_1 .$$

Now $\bar{a}_{ij}\bar{\varphi}_0 = \bar{c}_{ij}$ where $\bar{c}_{ij} \in W(\varepsilon_1, \ldots, \varepsilon_l)$, defined following Lemma 4.2.23. Then $\bar{a}_{ij}\bar{\varphi}_0\bar{\varphi}_1 = \xi_{ij}\bar{b} + \bar{c}_{ij}$ for some ξ_{ij} , and so $\bar{a}_{ij}\left(\bar{\varphi}_0\bar{\varphi}_1\bar{\varphi}_0^{-1}\right) = \xi_{ij}\bar{b} + \bar{a}_{ij}$. Similarly, $\bar{b}_{ij}\left(\bar{\varphi}_0\bar{\varphi}_1\bar{\varphi}_0^{-1}\right) = \eta_{ij}\bar{b} + \bar{b}_{ij}$. Since $\bar{\varphi}_0\bar{\varphi}_1\bar{\varphi}_0^{-1} \in QSp(U)$, ξ_{ij}, η_{ij} are of the appropriate forms. Hence $\bar{\varphi}_0\bar{\varphi}_1\bar{\varphi}_0^{-1} \in T_1$. $//$

4.3.4 LEMMA. T_1 *has cyclic centre of order* q^r .

Proof. It is easily verified that $\bar{\varphi}_\mu \in Z(T_1)$, where

$$\bar{a}\bar{\varphi}_\mu = \bar{a} + \mu\bar{b} , \quad \bar{b}\bar{\varphi}_\mu = \bar{b} ,$$

$$\bar{a}_{ij}\bar{\varphi}_\mu = \bar{a}_{ij} , \quad \bar{b}_{ij}\bar{\varphi}_\mu = \bar{b}_{ij} , \quad j = 1, \ldots, \varepsilon_i , \quad 1 \le i \le l ,$$

and that $\bar{\varphi}_\mu = \bar{\varphi}_1^{\mu}$, $|\bar{\varphi}_1| = q^r$.

The proof is then complete if we can show that $\bar{\varphi} \in Z(T_1)$ implies that $\bar{\varphi} = \bar{\varphi}_\mu$ for some μ . Suppose

$$\bar{a}\bar{\varphi} = \bar{a} + \mu\bar{b} + \bar{c} ,$$

where $\bar{c} = \sum_{i=1}^{r-1} \sum_{j=1}^{\varepsilon_i} (\mu_{ij}\bar{b}_{ij} - \sigma_{ij}\bar{a}_{ij}) + \sum_{i=r}^{l} \sum_{j=1}^{\varepsilon_i} q^{i-r}(\mu_{ij}\bar{b}_{ij} - \sigma_{ij}\bar{a}_{ij})$. We

are done if we can show that $\bar{c} = 0$.

Let $1 \le s \le l$, $1 \le t \le \varepsilon_s$, and define $\theta_{st} \in T_1$ as follows:

$$\bar{a}\bar{\theta}_{st} = \bar{a} + \nu_{st}\bar{b}_{st} \ , \quad \bar{b}\bar{\theta}_{st} = \bar{b} \ ,$$

where

$$\nu_{st} = \begin{cases} 1 & \text{if } 1 \le s < r \ , \\ q^{s-r} & \text{if } r \le s \le l \ , \end{cases}$$

$$\bar{a}_{st}\bar{\theta}_{st} = \begin{cases} q^{r-s}\bar{b} + \bar{a}_{st} & \text{if } 1 \le s < r \ , \\ \bar{b} + \bar{a}_{st} & \text{if } r \le s \le l \ , \end{cases}$$

$$\bar{a}_{ij}\bar{\theta}_{st} = \bar{a}_{ij} \quad \text{if } i \ne s \text{ or } j \ne t \ ,$$

$$\bar{b}_{ij}\bar{\theta}_{st} = \bar{b}_{ij} \quad \text{for all } i, j \ .$$

We have $\bar{a}(\bar{\varphi}\bar{\theta}_{st}) = \bar{a} + \nu_{st}\bar{b}_{st} + \mu\bar{b} + \bar{c}\bar{\theta}_{st}$, and $\bar{a}(\bar{\theta}_{st}\bar{\varphi}) = \bar{a} + \mu\bar{b} + \bar{c} + \nu_{st}\bar{b}_{st}\bar{\varphi}$. Thus $\nu_{st}\bar{b}_{st} + \bar{c}\bar{\theta}_{st} = \bar{c} + \nu_{st}\bar{b}_{st}\bar{\varphi}$. Now

$$\bar{c}\bar{\theta}_{st} = \begin{cases} -q^{r-s}\sigma_{st}\bar{b} + \bar{c} & \text{if } 1 \le s < r \ , \\ -q^{s-r}\sigma_{st}\bar{b} + \bar{c} & \text{if } r \le s \le l \ , \end{cases}$$

$$\bar{b}_{st}\bar{\varphi} = \begin{cases} q^{r-s}\sigma_{st}\bar{b} + \bar{b}_{st} & \text{if } 1 \le s < r \ , \\ \sigma_{st}\bar{b} + \bar{b}_{st} & \text{if } r \le s \le l \ . \end{cases}$$

Hence if $1 \le s < r$, we have $q^{r-s}\sigma_{st}(1+\nu_{st})\bar{b} = 0$, or $2\sigma_{st} \equiv 0 \pmod{q^s}$ and so $\sigma_{st} = 0$ since q is odd. However, if $r \le s \le l$, we have $2q^{r-s}\sigma_{st}\bar{b} = 0$, and so $q^{s-r}\sigma_{st} = 0$. Thus we have shown that in the expression for $\bar{c}$, the coefficients of the $\bar{a}_{ij}$ are all zero.

By considering $\bar{\psi}_{st} \in T_1$, where

$$\bar{a}\bar{\psi}_{st} = \bar{a} - \nu_{st}\bar{a}_{st} \ , \quad \bar{b}\bar{\psi}_{st} = \bar{b} \ ,$$

with ν_{st} defined as before,

$$\bar{a}_{ij}\bar{\psi}_{st} = \bar{a}_{ij} \quad \text{for all} \quad i, j \ ,$$

$$\bar{b}_{st}\bar{\psi}_{st} = \begin{cases} q^{r-s}\bar{b} + \bar{b}_{st} & \text{if} \quad 1 \leq s < r \ , \\ \\ \bar{b} + \bar{b}_{st} & \text{if} \quad r \leq s \leq l \ , \end{cases}$$

$$\bar{b}_{ij}\bar{\psi}_{st} = \bar{b}_{ij} \quad \text{if} \quad i \neq s \quad \text{or} \quad j \neq t \ ,$$

we can likewise show that the coefficients of the $\bar{b}_{ij}$ are also all zero. Hence $\bar{c} = 0$. //

4.3.5 LEMMA. *T_1 is of class 2 .*

Proof. Let $\bar{\varphi}, \bar{\varphi}' \in T_1$ and

$$\bar{a}_{ij}\bar{\varphi} = \xi_{ij}\bar{b} + \bar{a}_{ij} \ , \quad \bar{a}_{ij}\bar{\varphi}' = \xi'_{ij}\bar{b} = \bar{a}_{ij} \ ,$$

so that $\bar{a}_{ij}\bar{\varphi}^{-1} = -\xi_{ij}\bar{b} + \bar{a}_{ij}$, $\bar{a}_{ij}\bar{\varphi}'^{-1} = -\xi'_{ij}\bar{b} + \bar{a}_{ij}$. It is easily verified that $\bar{a}_{ij}[\bar{\varphi}, \bar{\varphi}'] = \bar{a}_{ij}$. Similarly $\bar{b}_{ij}[\bar{\varphi}, \bar{\varphi}'] = \bar{b}_{ij}$. Hence $\bar{a}[\bar{\varphi}, \bar{\varphi}'] = \bar{a} + \mu\bar{b}$ for some μ , and so $[\bar{\varphi}, \bar{\varphi}\,] \in Z(T_1)$. //

4.3.6 LEMMA. *Let $0 \leq k < r$. Then*

$$\log_q |\Omega_k(T_1)| = r - k + 2 \sum_{i=k+1}^{r-1} (i-k)\varepsilon_i + 2 \sum_{i=r}^{l} (r-k)\varepsilon_i \ ,$$

where $\Omega_k(T_1)$ is the subgroup generated by the q^k-th powers of elements of T_1 , and $\Omega_0(T_1) = T_1$.

Proof. Since T_1 is of class 2 , $(\bar{\varphi}\bar{\psi})^{q^k} = \bar{\varphi}^{q^k}\bar{\psi}^{q^k}[\bar{\psi}, \bar{\varphi}]^{\binom{q^k}{2}}$,

and hence $\Omega_k(T_1) = \left\{\bar{\varphi}^{q^k} : \bar{\varphi} \in T_1\right\}$.

We make two elementary observations. Firstly, if $\bar{a}\bar{\varphi} = \bar{a} + \mu\bar{b} + \bar{c}$, then $\bar{c}\bar{\varphi} = \bar{c}$. This is easily checked. Secondly, if $\bar{x}\bar{\varphi}^{q^i} = \bar{x}$ for a fixed $\bar{x} \in U$ and a fixed positive integer i ,

then $\bar{x}\bar{\varphi}^{q^j} = \bar{x}$ for $j \geq i$. This is shown by induction on j:

$$\bar{x}\bar{\varphi}^{q^{j+1}} = \left(\bar{x}\bar{\varphi}^{q^j}\right)\bar{\varphi}^{q^{j+1}-q^j} = \bar{x}\left(\bar{\varphi}^{q^j}\right)^{q-1} = \bar{x} .$$

It follows that $\Omega_k(T_1)$ consists of isometries of the form

$$\bar{a}\bar{\theta} = \bar{a} + \mu q^k \bar{b} + a^k \bar{c} , \quad \bar{b}\bar{\theta} = \bar{b} ,$$

$$\bar{a}_{ij}\bar{\theta} = \bar{a}_{ij} , \quad \bar{b}_{ij}\bar{\theta} = \bar{b}_{ij} , \quad j = 1, \ldots, \varepsilon_i , \quad 1 \leq i \leq k ,$$

$$\left.\begin{aligned} \bar{a}_{ij}\bar{\theta} &= \mu_{ij} q^{r-i+k}\bar{b} + \bar{a}_{ij} \\ \bar{b}_{ij}\bar{\theta} &= \sigma_{ij} q^{r-i+k}\bar{b} + \bar{b}_{ij} \end{aligned}\right\} \quad j = 1, \ldots, \varepsilon_i , \quad k < i < r ,$$

$$\left.\begin{aligned} \bar{a}_{ij}\bar{\theta} &= \mu_{ij} q^{k}\bar{b} + \bar{a}_{ij} \\ \bar{b}_{ij}\bar{\theta} &= \sigma_{ij} q^{k}\bar{b} + \bar{b}_{ij} \end{aligned}\right\} \quad j = 1, \ldots, \varepsilon_i , \quad r \leq i \leq l .$$

An easy enumeration gives the required order. //

4.3.7 LEMMA. $T_1 \cong Q(r)^{\varepsilon_l + \ldots + \varepsilon_r} Q(r-1)^{\varepsilon_{r-1}} \ldots Q(1)^{\varepsilon_1}$.

Proof. By Lemmas 4.3.4 and 4.3.5, T_1 is a finite q-group of class 2, with cyclic centre of order q^r. Evidently T_1 is of exponent q^r. The canonic decomposition of T_1 is then either $Q(r)^{\delta_r} \ldots Q(1)^{\delta_1}$, $\delta_r > 0$, or

$$Q(n_1', r_1') \ldots Q(n_\beta', r_\beta')Q(k)^{\delta_k} \ldots Q(1)^{\delta_r} , \quad n_1' = r .$$

We show that the latter decomposition is not possible. Suppose T_1 has the second decomposition. Then by Lemma 4.2.9, $Z(T_1)$ has order $q^{m'}$ where $m' = \max\{k, r_1', n_\beta' - r_\beta'\}$. Since $k < n_1'$, $r_1' < n_1'$, $n_\beta' - r_\beta' \leq n_\beta'$, we must have $\beta = 1$, $r_1' = 0$. We would then have $|\Omega_{r-1}(T_1)| = q$, contradicting Lemma 4.3.6 which gives $|\Omega_{r-1}(T_1)| > q$ since $\varepsilon_l > 0$. Hence $T_1 \cong Q(r)^{\delta_r} \ldots Q(1)^{\delta_1}$, and so

$$\log_q|\Omega_k(T_1)| = r - k + 2\sum_{i=k+1}^{r}(i-k)\delta_i \quad \text{for} \quad 0 \le k \le r .$$

Equating this with the expression in Lemma 4.3.6, we get the values of δ_i in terms of the ε_i as desired. //

The case when $l < r$. $QSp(U)$ is then the group of isometries of the form:

$$\left.\begin{aligned} \bar{a}\bar{\varphi} &= \bar{a} + \mu\bar{b} + \bar{c} \\ \bar{b}\bar{\varphi} &= \bar{b} \end{aligned}\right\}$$

$$\left.\begin{aligned} \bar{a}_{ij}\bar{\varphi} &= \mu_{ij}q^{r-i}\bar{b} + \bar{c}_{ij} \\ \bar{b}_{ij}\bar{\varphi} &= \sigma_{ij}q^{r-i}\bar{b} + \bar{d}_{ij} \end{aligned}\right\} \quad j = 1, \ldots, \varepsilon_i , \quad 1 \le i \le l .$$

As in the previous case, we define the corresponding subgroups T_0, T_1 of $QSp(U)$ in a similar way: $T_0 = \{\bar{\varphi} \in QSp(U) : \bar{a}\bar{\varphi} = \bar{a} , \ \bar{b}\bar{\varphi} = \bar{b}\}$, and T_1 is the group of isometries of the form

$$\left.\begin{aligned} \bar{a}\bar{\varphi} &= \bar{a} + \bar{b} + \bar{c} \\ \bar{b}\bar{\varphi} &= \bar{b} \end{aligned}\right\}$$

$$\left.\begin{aligned} \bar{a}_{ij}\bar{\varphi} &= \mu_{ij}q^{r-i}\bar{b} + \bar{a}_{ij} \\ \bar{b}_{ij}\bar{\varphi} &= \sigma_{ij}q^{r-i}\bar{b} + \bar{b}_{ij} \end{aligned}\right\} \quad j = 1, \ldots, \varepsilon_i , \quad 1 \le i \le l .$$

Lemmas 4.3.2-4.3.5 remain valid for this new subgroup T_1 . This is easily proved with obvious modifications to their proofs. We now complete the proof of Theorem 4.3.1 *(ii)* by proving the following two lemmas. (Note that $\Omega_k(T_1)$ is defined as in Lemma 4.3.6.)

4.3.8 LEMMA. *Let* $0 \le k \le l$. *Then*

$$\log_q|\Omega_k(T_1)| = r - k + 2\sum_{i=k+1}^{l}(i-k)\varepsilon_i .$$

Proof. With reference to the preliminary remarks in the proof of Lemma 4.3.6, we conclude that $\Omega_k(T_1)$ is the set of isometries of the form

$$\bar{a}\bar{\theta} = \bar{a} + \mu q^{k}\bar{b} + q^{k}\bar{c} \ , \quad \bar{b}\bar{\theta} = \bar{b} \ ,$$

$$\bar{a}_{ij}\bar{\theta} = \bar{a}_{ij} \ , \quad \bar{b}_{ij}\bar{\theta} = \bar{b}_{ij} \ , \quad j = 1, \ldots, \varepsilon_i \ , \quad 1 \leq i \leq k \ ,$$

$$\left.\begin{aligned} \bar{a}_{ij}\bar{\theta} &= \mu_{ij}q^{r-i+k}\bar{b} + \bar{a}_{ij} \\ \bar{b}_{ij}\bar{\theta} &= \sigma_{ij}q^{r-i+k}\bar{b} + \bar{b}_{ij} \end{aligned}\right\} \ j = 1, \ldots, \varepsilon_i \ , \quad k < i \leq l \ . \qquad //$$

4.3.9 LEMMA. $T_1 \cong Q(r, 0)Q(l)^{\varepsilon_l} \ldots Q(1)^{\varepsilon_1}$.

Proof. Since T_1 is a finite q-group of exponent q^r and class 2 with cyclic centre of order q^r, the canonic decomposition of T_1 is either $Q(r)^{\delta_r} \ldots Q(1)^{\delta_1}$, $\delta_r > 0$, or $Q(n_1', r_1') \ldots Q(n_\beta', r_\beta')Q(k)^{\delta_k} \ldots Q(1)^{\delta_1}$, $n_1' = r$. If T_1 has the first decomposition, then clearly

$$\log_q|\Omega_l(T_1)| = r - l + 2\sum_{i=l+1}^{r}(i-l)\delta_i > r - l \ ,$$

contradicting Lemma 4.3.8 (with $k = l$). Hence T_1 has the second decomposition. By considering $|Z(T_1)|$ as we did in the proof of Lemma 4.3.7, we have $T_1 \cong Q(r, 0)Q(k)^{\delta_k} \ldots Q(1)^{\delta_1}$, $\delta_k > 0$. If $k > l$, then $\log_q|\Omega_l(T_1)| > r - l$, while if $k < l$, then $\log_q|\Omega_k(T_1)| = r - k$; both instances contradicting Lemma 4.3.8. Hence $k = l$. Finally a comparison of $|\Omega_k(T_1)|$ with that in Lemma 4.3.8 gives the required result. //

CHAPTER 5

THE CREAM PROBLEM FOR SUBVARIETIES OF $\underline{\underline{A}}_r(\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_s)$

The object of this chapter is to study the CREAM problem for subvarieties of $\underline{\underline{A}}_r(\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_s)$ where r, s are coprime integers with s odd and not divisible by q^4 for any prime q. We will show that this has an affirmative solution. We will also give an example of an infinite (but not closed) class $\underline{\underline{S}}$ of irreducible linear groups in $\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_{q^4}$, q odd, for which the function $n \mapsto c_{\underline{\underline{S}}}(n)$, $n \in N^+$, (see 2.1), is not the restriction of a CREAM function.

5.1 The infinite closed classes

In this section we introduce a convenient way of keeping track of the infinite classes of irreducible linear groups of a fixed exponent. This will be useful in 5.3. Denote the closed class of all irreducible linear groups in $\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_{q^i}$ by $\underline{\underline{Q}}_i$, q odd. We will use the notations of Chapter 2 and write $Q(k) = Q(k, k)$. Let $n > 1$ be a fixed integer. Suppose $\underline{\underline{X}} \leq \underline{\underline{Q}}_n$ is a closed class not contained in $\underline{\underline{Q}}_{n-1}$. Define the following (not necessarily closed) classes of linear groups:

$$\underline{\underline{S}}_i = \underline{\underline{X}} \cap Q(n, i)\underline{\underline{Q}}_{n-1}, \quad i = 0, 1, \ldots, n-1,$$

$$\underline{\underline{S}}^j = \underline{\underline{X}} \cap Q(n)^j\underline{\underline{Q}}_{n-1}, \quad j = 0, 1, \ldots,$$

where $X\underline{\underline{Q}}_{n-1}$ denotes the set of central products with cyclic centres of X and Y for each $Y \in \underline{\underline{Q}}_{n-1}$ and $X = Q(n, i)$ or $Q(n)^j$. We call the $\underline{\underline{S}}_i$, $\underline{\underline{S}}^j$ the *derived classes* of $\underline{\underline{X}}$. Note that $\underline{\underline{S}}^0$ is closed.

We classify the derived classes as follows. We say that the *rank* of $\underline{\underline{S}}_i$ is 0 if $\underline{\underline{S}}_i$ is finite (or empty); that the *rank* of $\underline{\underline{S}}_i$ is 1 if $Q(n, i)Q(1)^{\varepsilon_1} \in \underline{\underline{S}}_i$ for all $\varepsilon_1 = 0, 1, \ldots$, but $Q(n, i)Q(2)^{\varepsilon_2} \notin \underline{\underline{S}}_i$ for some $\varepsilon_2 > 0$; and in general, that the *rank*

of $\underline{\underline{S}}_i$ is k, where $1 \leq k < n$, if $Q(n, i)Q(k)^{\varepsilon_k} \ldots Q(1)^{\varepsilon_1} \in \underline{\underline{S}}_i$ for all $\varepsilon_1, \ldots, \varepsilon_k = 0, 1, \ldots$, but $Q(n, i)Q(k+1)^{\varepsilon_{k+1}} \notin \underline{\underline{S}}_i$ for some $\varepsilon_{k+1} > 0$. Likewise, for each $j > 0$, we say that the *rank* of $\underline{\underline{S}}^j$ is 0 if $\underline{\underline{S}}^j$ is finite (or empty); and that the *rank* of $\underline{\underline{S}}^j$ is k, where $1 \leq k < n$, if $Q(n)^j Q(k)^{\varepsilon_k} \ldots Q(1)^{\varepsilon_1} \in \underline{\underline{S}}^j$ for all $\varepsilon_1, \ldots, \varepsilon_k = 0, 1, \ldots$, but $Q(n)^j Q(k+1)^{\varepsilon_{k+1}} \notin \underline{\underline{S}}^j$ for some $\varepsilon_{k+1} > 0$. Note that $\underline{\underline{S}}^0$ consists of linear groups in $\underline{\underline{O}}_{n-1}$ and so we do not define the rank of $\underline{\underline{S}}^0$.

We will find the following observations useful, and the results of 3.2 will be freely used.

5.1.1 LEMMA.

(i) If rank of $\underline{\underline{S}}_0 = k > 0$, *then rank of* $\underline{\underline{S}}_i = k$ *for* $i = 0, 1, \ldots, k$.

(ii) The following chain of inequalities holds:

rank of $\underline{\underline{S}}_0 \geq$ *rank of* $\underline{\underline{S}}_1 \geq \ldots \geq$ *rank of* $\underline{\underline{S}}_{n-1} \geq$ *rank of* $\underline{\underline{S}}^1 \geq$ *rank of* $\underline{\underline{S}}^2 \geq \ldots$.

Proof. *(i)* Since $\underline{\underline{S}}_0$ has rank $k > 0$, $Q(n, 0)Q(k)^{\varepsilon_k} \ldots Q(1)^{\varepsilon_1} \in \underline{\underline{S}}_0$ for all $\varepsilon_1, \ldots, \varepsilon_k = 0, 1, \ldots$. It is clear that if $0 \leq i \leq k$, $Q(n, i)Q(k)^{\varepsilon_k} \ldots Q(1)^{\varepsilon_1} \in \underline{\underline{X}}$ for all $\varepsilon_1, \ldots, \varepsilon_k = 0, 1, \ldots$, and hence are in $\underline{\underline{S}}_i$. Moreover if $Q(n, i)Q(k+1)^{\varepsilon_{k+1}} \in \underline{\underline{S}}_i$ for all $\varepsilon_{k+1} = 0, 1, \ldots$, then $Q(n, 0)Q(k+1)^{\varepsilon_{k+1}} \in \underline{\underline{S}}_0$ for all $\varepsilon_{k+1} = 0, 1, \ldots$, which is not so. Hence $\underline{\underline{S}}_i$ has rank k.

(ii) Let $0 \leq i < n$. Suppose rank of $\underline{\underline{S}}_i = k_i$. Then rank of

$\underline{\underline{S}}_{i+1}$ cannot be greater than k_i . Otherwise $Q(n, i+1)Q(l)^{\varepsilon_l} \in \underline{\underline{S}}_{i+1}$ for all $\varepsilon_l = 0, 1, \ldots$, where $l = k_i + 1$, and since $Q(n, i) \prec Q(n, i+1)$, it follows that $Q(n, i)Q(l)^{\varepsilon_l} \in \underline{\underline{S}}_i$ for all $\varepsilon_l = 0, 1, \ldots$, which is a contradiction. In the same way, we can easily prove: rank of $\underline{\underline{S}}_{n-1} \geq$ rank of $\underline{\underline{S}}^1 \geq \ldots$. //

The next lemma is immediate.

5.1.2 LEMMA. $\underline{\underline{X}} = \left(\bigcup_{i=0}^{n-1} \underline{\underline{S}}_i \right) \cup \left(\bigcup_{j=0}^{\nu} \underline{\underline{S}}^j \right)$, *where* ν *is the index of* $\underline{\underline{X}}$ *(see* 3.3*), and the union is disjoint.*

We now give a detailed description of the derived classes in some simple cases. This will be required in 5.3.

5.1.3 LEMMA. *Suppose* $\underline{\underline{X}} \leq \underline{\underline{Q}}_2$ *is a closed class not contained in* $\underline{\underline{Q}}_1$. *The derived classes of* $\underline{\underline{X}}$ *of rank* 1 *are of the forms*

$$\underline{\underline{S}}_0 = \{Q(2, 0)Q(1)^r : r = 0, 1, \ldots\} ,$$

$$\underline{\underline{S}}_1 = \{Q(2, 1)Q(1)^r : r = 0, 1, \ldots\} ,$$

$$\underline{\underline{S}}^j = \{Q(2)^j Q(1)^r : r = 0, 1, \ldots\} , \quad j > 0 .$$

Proof. The irreducible linear groups of exponent q^2 are $Q(2, 0)Q(1)^r$, $Q(2, 1)Q(1)^r$, $Q(2)^j Q(1)^r$, $j > 0$, $r \geq 0$. //

5.1.4 LEMMA. *Suppose* $\underline{\underline{X}} \leq \underline{\underline{Q}}_3$ *is a closed class not contained in* $\underline{\underline{Q}}_2$. *The derived classes of* $\underline{\underline{X}}$ *of rank* 1 *are of the forms*

$$\underline{\underline{S}}_i = \bigcup_{s=0}^{\sigma_i} \underline{\underline{R}}_{i,s} , \quad 0 \leq \sigma_i < \infty , \quad i = 0, 1, 2 ,$$

$$\underline{\underline{S}}^j = \bigcup_{s=0}^{\mu_j} \underline{\underline{R}}^{(j,s)} , \quad 0 \leq \mu_j < \infty , \quad j > 0 ,$$

where

$$\underline{\underline{R}}_{i,0} = \{Q(3, i)Q(1)^r : r = 0, 1, \ldots\} , \quad i = 0, 1, 2 ,$$

$$\underline{\underline{R}}_{i,s} = \left\{Q(3, i)Q(2)^s Q(1)^r : r = 0, 1, \ldots , \rho_{is} \leq \infty\right\} ,$$

$$0 < s \leq \sigma_i , \quad i = 0, 1, 2 ,$$

$$\underline{\underline{R}}^{(j,0)} = \{Q(3)^j Q(1)^r : r = 0, 1, \ldots\} , \quad j > 0 ,$$

$$\underline{\underline{R}}^{(j,s)} = \left\{Q(3)^j Q(2)^s Q(1)^r : r = 0, 1, \ldots , \lambda_{js} \leq \infty\right\} ,$$

$$0 < s \leq \mu_j , \quad j > 0 .$$

The derived classes of $\underline{\underline{X}}$ *of rank* 2 *are of the forms*

$$\underline{\underline{S}}_i = \{Q(3, i)Q(2)^s Q(1)^r : r, s = 0, 1, \ldots\} , \quad i = 0, 1, 2 ,$$

$$\underline{\underline{S}}^j = \{Q(3)^j Q(2)^s Q(1)^r : r, s = 0, 1, \ldots\} , \quad j > 0 .$$

Proof. It is clear from Chapter 2 that the irreducible linear groups of exponent q^3 are

$$Q(3, i)Q(2)^s Q(1)^r , \quad Q(3)^j Q(2)^s Q(1)^r ,$$

$$i = 0, 1, 2 , \quad j > 0 , \quad r, s \geq 0 .$$

If the derived class $\underline{\underline{S}}_i$ has rank 1, then by definition, there exists a unique largest integer $\sigma_i \geq 0$ for which $Q(3, i)Q(2)^{\sigma_i} \in \underline{\underline{S}}_i$. If $\sigma_i > 0$, we define ρ_{is} for each $0 < s \leq \sigma_i$, to be the largest integer for which $Q(3, i)Q(2)^s Q(1)^{\rho_{is}} \in \underline{\underline{S}}_i$. Note that ρ_{is} may be infinite. Similarly for $\underline{\underline{S}}^j$, $j > 0$, of rank 1. The forms of the derived classes of rank 2 are obvious. //

5.1.5 LEMMA. *Suppose* $\underline{\underline{X}} \leq \underline{\underline{O}}_2$ *is a closed class not contained in* $\underline{\underline{O}}_1$. *If the derived class* $\underline{\underline{S}}_0$ *has rank* 1, *then* $\underline{\underline{S}}^0 \cup \underline{\underline{S}}_0 \cup \underline{\underline{S}}_1$ *is the class of all irreducible linear groups in* $\underline{\underline{A}}_{q^2} \vee (\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_q)$.

Proof. $\underline{\underline{S}}^0 = \underline{\underline{O}}_1$, $\underline{\underline{S}}_i = \{Q(2, i)Q(1)^r : r = 0, 1, \ldots\}$, $i = 0, 1$. //

5.1.6 LEMMA. *Suppose* $\underline{\underline{X}} \leq \underline{\underline{O}}_3$ *is a closed class not contained*

in $\underline{\underline{Q}}_2$. *If the derived class* $\underline{\underline{S}}_0$ *has rank* 2 , *then* $\underline{\underline{S}}^0 \cup \left(\bigcup_{i=0}^{2} \underline{\underline{S}}_i \right)$ *is the class of all irreducible linear groups in* $\underline{\underline{A}}_{q^3} \vee (\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_{q^2})$.

Proof. Clearly $\underline{\underline{S}}^0 = \underline{\underline{Q}}_2$, and $\underline{\underline{S}}_i$, $i = 0, 1, 2$, are given by Lemma 5.1.4. Evidently the union of these classes gives all the irreducible linear groups in the stated variety. //

5.2 Some calculations of $c_n(X)$

We will use the notations of 1.2 and 5.1 except that we write $c_n(\underline{\underline{X}}) = c_{\underline{\underline{X}}}(n)$ and $k_n(G) = k_G(n)$. It is clear from 3.1 that we need only consider irreducible linear groups over a splitting field. For every $X \in \underline{\underline{Q}}_i$, we denote the degree of X by deg X . By Corollary 1.3.13,

$$c_n(X) = (\deg X)^2 k_n(X)/|\text{lin aut } X| .$$

For every $X \in \underline{\underline{Q}}_3$, $c_n(X)$ will be explicitly calculated. We denote the q^i-cycle by C_i and write $C_iC_j = C_i \times C_j$, $C_i^k = C_iC_i^{k-1}$, $k \geq 2$.

First some calculations on deg X .

5.2.1 LEMMA.

(i) For $n \geq r \geq 0$, $\deg Q(n, r) = q^r$.

(ii) Suppose XY *is a central product with cyclic centre of* $X, Y \in \underline{\underline{Q}}_i$. *Then* $\deg(XY) = \deg X \,.\, \deg Y$.

Proof. *(i)* Since we are working in a splitting field, the result is trivial if $r = 0$. So suppose $r > 0$. We may also assume that the field contains a primitive q^r-th root of unity, ξ say. Then it is easily checked that

$$a = \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & & 1 \\ 1 & & & 0 \end{pmatrix} , \quad b = \begin{pmatrix} 1 & & & \\ & \xi & & \\ & & \ddots & \\ & & & \xi^{q^r-1} \end{pmatrix}$$

gives a matrix representation of $Q(r, r)$ so that $\deg Q(r, r) = q^r$. Since $Q(n, 0)Q(n, r) = Q(n, 0)Q(r, r)$ by Lemma 2.2.4, it follows that $\deg Q(n, r) = q^r$.

(ii) If $XY = X$, then Y is cyclic, and so the assertion follows from *(i)*. Now suppose $XY \neq X$ or Y. Let U and V be the vector spaces on which X and Y act respectively. Then $U \# V$ is the space on which XY acts, by Lemma 3.2.4. It then follows from 9.11, Chapter V, Huppert [16], that $\dim(U \# V) = \dim U \cdot \dim V$, where $\dim U$, $\dim V$ denote the dimensions of the vector spaces U, V respectively. //

The next lemma is a special case of a theorem of Gaschütz [8]; an independent proof is easily given. As we will see, this lemma reduces the calculation of $k_n(X)$ to that of $k_n\left(C_1^i\right)$.

5.2.2 LEMMA. *Suppose G is a finite group and $H \triangleleft G$, $H \leq \Phi(G)$. Then $k_n(G) = |H|^n k_n(G/H)$.*

Proof. Define the relation $\sim$ on the n-tuples of elements of G as follows:

$\underline{x} \sim \underline{y}$ if and only if $x_i = y_i h_i$ for some $h_i \in H$, $i = 1, \ldots, n$, where $\underline{x} = (x_1, \ldots, x_n)$, $\underline{y} = (y_1, \ldots, y_n)$. Then $\sim$ is an equivalence relation. Now G is generated modulo H by $x_1, \ldots, x_n$ if and only if G is generated by $x_1, \ldots, x_n$. Hence we can define the following correspondence θ between the equivalence classes (defined by $\sim$ on the n-tuples of elements which generate G) and the n-tuples of elements which generate G/H,

$$\theta : [\underline{x}] \mapsto (x_1 H, \ldots, x_n H),$$

where $\underline{x} = (x_1, \ldots, x_n)$ is a representative of the equivalence class $[\underline{x}]$. Clearly θ is independent of the choice of $\underline{x}$. Moreover θ is one-to-one and onto. Thus there are exactly as many equivalence classes as there are n-tuples of elements which generate G/H. But each equivalence class contains exactly $|H|$ distinct elements. //

To calculate $k_n\left(C_1^i\right)$ we will again need a theorem of Gaschütz.

5.2.3 THEOREM (Gaschütz [8]). *If H is a minimal soluble normal subgroup of the finite group G, then*

$$k_n(G) = k_n(G/H).\left(|H|^n - c\right) ,$$

where c is the number of complements of H in G.

5.2.4 THEOREM. *For $m \geq 1$,* $k_n\left(C_1^m\right) = (q^n - q^{m-1})k_n\left(C_1^{m-1}\right)$.

Proof. Consider C_1^m as a vector space V of dimension m over $GF(q)$,

$$V = \langle v_1 \rangle \oplus \ldots \oplus \langle v_m \rangle .$$

We calculate the number of complements of $\langle v_1 \rangle$ in V. Let

$$A = \{\alpha \in \text{aut } V : v_1\alpha = \lambda v_1 \text{ for some } 0 \neq \lambda \in GF(q)\} .$$

Then A is evidently a subgroup and consists of linear transformations of V of the form

$$v_1\alpha = \lambda_1 v_1 \quad , \quad \lambda_1 \neq 0 ,$$

$$v_i\alpha = \lambda_i v_1 + u_i \quad , \quad i = 2, \ldots, m ,$$

where $\lambda_1, \ldots, \lambda_m \in GF(q)$, $u_2, \ldots, u_m \in U = \langle v_2, \ldots, v_m \rangle$. It is easily checked that $u_2, \ldots, u_m$ are linearly independent. Hence

$$|A| = (q-1)q^{m-1}|GL(m-1, q)| .$$

Let $\Omega = \{W \leq V : V = \langle v_1 \rangle \oplus W\}$. For every $\alpha \in A$, $W \in \Omega$, we have $V = V\alpha = \langle v_1 \rangle + W\alpha$. In fact $\langle v_1 \rangle \cap W\alpha = 0$; otherwise $v_1 \in W\alpha$ implies that $V = W\alpha$. Hence $V = \langle v_1 \rangle \oplus W\alpha$. For any two $W, W' \in \Omega$, there exists $\alpha \in A$ such that $W\alpha = W'$. We merely define α as follows:

$$v_1\alpha = v_1 \quad , \quad w_i\alpha = w_i' \quad , \quad i = 2, \ldots, m ,$$

where $\{w_2, \ldots, w_m\}$, $\{w_2', \ldots, w_m'\}$ are bases of W, W' respectively. Hence A acts transitively on Ω and so $|A| = |A_0|.|\Omega|$, where

$$A_0 = \{\alpha \in A : W_0\alpha = W_0 \text{ and } W_0 = \langle v_2, \ldots, v_m \rangle\} .$$

Plainly A_0 consists of all those $\alpha \in A$ for which $\lambda_2, \ldots, \lambda_m$ are zero. Hence

$$|A_0| = (q-1)|GL(m-1, q)| ,$$

and so $|\Omega| = q^{m-1}$. The lemma then follows from Theorem 5.2.3. //

5.2.5 COROLLARY. *For* $m \geq 1$, $k_n\left(C_1^m\right) = q^{\frac{1}{2}m(m-1)} \prod_{i=1}^{m} (q^{n-i+1}-1)$.

In the next four lemmas, we will assume that $n_1 > l > 0$, $\varepsilon_l > 0$ and write $\lambda = 2\sum_{i=1}^{l} \varepsilon_i$, $\mu = 2\sum_{i=1}^{l} (i-1)\varepsilon_i$. In Lemmas 5.2.7 and 5.2.9, δ_{l,n_1-1} is the Kronecker delta.

5.2.6 LEMMA.

(i) $k_n\left(Q(l)^{\varepsilon_l} \ldots Q(1)^{\varepsilon_1}\right) = q^{(l+\mu)n} k_n\left(C_1^{\lambda}\right)$.

(ii) $k_n\left(Q(n_1, 0)Q(l)^{\varepsilon_l} \ldots Q(1)^{\varepsilon_1}\right) = q^{(n_1-1+\mu)n}(q^n-q^{\lambda})k_n\left(C_1^{\lambda}\right)$.

(iii) $k_n\left(Q(n_1, 1)Q(l)^{\varepsilon_l} \ldots Q(1)^{\varepsilon_1}\right) = q^{(n_1-1+\mu)n}(q^n-q^{1+\lambda})(q^n-q^{\lambda})k_n\left(C_1^{\lambda}\right)$.

(iv) $k_n\left(Q(n_1, n_1-1)Q(l)^{\varepsilon_l} \ldots Q(1)^{\varepsilon_1}\right) = q^{(3n_1-5+\mu)n} \times (q^n-q^{1+\lambda})(q^n-q^{\lambda})k_n\left(C_1^{\lambda}\right)$.

Proof. *(i)* Put $X = Q(l)^{\varepsilon_l} \ldots Q(1)^{\varepsilon_1}$ so that $|X'| = q^l$ and

$$\overline{X} = X/X' \cong C_l^{2\varepsilon_l} \ldots C_1^{2\varepsilon_1} .$$

By Lemma 5.2.2, $k_n(X) = q^{ln}k_n(\overline{X})$. Now put

$$\overline{N} = \langle \bar{x}^q : \bar{x} \in \overline{X} \rangle \leq \Phi(\overline{X}) ,$$

so that $|\overline{N}| = q^{\mu}$ and $\overline{X}/\overline{N} \cong C_1^{\lambda}$. Hence by Lemma 5.2.2,

$$k_n(\overline{X}) = q^{\mu n}k_n\left(C_1^{\lambda}\right) .$$

(ii) Put $X = Q(n_1, 0)Q(l)Q(l)^{\varepsilon_l} \ldots Q(1)^{\varepsilon_1}$ so that $|X'| = q^l$ and

$$\overline{X} = X/X' \cong C_{n_1-l}C_l^{2\varepsilon_l} \ldots C_1^{2\varepsilon_1} .$$

By Lemma 5.2.2, $k_n(X) = q^{ln}k_n(\overline{X})$. Now put

$$\overline{N} = \langle \bar{x}^q : \bar{x} \in \overline{X} \rangle \leq \Phi(\overline{X}) ,$$

so that $|\overline{N}| = q^{n_1-l-1+\mu}$ and $\overline{X}/\overline{N} \cong C_1^{1+\lambda}$. Hence by Lemma 5.2.2 and 5.2.4,

$$\begin{aligned} k_n(\overline{X}) &= |\overline{N}|^n k_n\left(C_1^{1+\lambda}\right) \\ &= |\overline{N}|^n (q^n - q^\lambda) k_n\left(C_1^\lambda\right) . \end{aligned}$$

(iii) and *(iv)*. Similar to *(ii)*. We merely note that if we write

$$X = Q(n_1, 1)Q(l)^{\varepsilon_l} \ldots Q(1)^{\varepsilon_1} , \quad Y = Q(n_1, n_1-1)Q(l)^{\varepsilon_l} \ldots Q(1)^{\varepsilon_1} ,$$

then $|X'| = q^l$, $X/X' \cong C_{n_1-l}C_1C_l^{2\varepsilon_l} \ldots C_1^{2\varepsilon_1}$, and $|Y'| = q^{n_1-1}$, $Y/Y' \cong C_{n_1-1}^2C_l^{2\varepsilon_l} \ldots C_1^{2\varepsilon_1}$. //

In the following lemma $Sp(\varepsilon_1, \ldots, \varepsilon_l)$ is the group in Chapter 4 and its order is given in Theorem 4.2.6.

5.2.7 LEMMA.

(i) $|\text{lin aut}(Q(l)^{\varepsilon_l} \ldots Q(1)^{\varepsilon_1})| = |\text{lin aut}(Q(n_1, 0)Q(l)^{\varepsilon_l} \ldots Q(1)^{\varepsilon_1})|$

$$= q^\lambda |Sp(\varepsilon_1, \ldots, \varepsilon_l)| .$$

(ii) $|\text{lin aut}(Q(n_1, 1)Q(l)^{\varepsilon_l} \ldots Q(1)^{\varepsilon_1})| = q^{3+2\lambda}|Sp(\varepsilon_1, \ldots, \varepsilon_l)| .$

(iii) $|\text{lin aut}(Q(n_1, n_1\text{-}1)Q(l)^{\varepsilon_l} \ldots Q(1)^{\varepsilon_1})| =$

$$q^{5n_1+3\lambda+2\mu-7-2\varepsilon_l\delta_{l,n_1-1}} \times |Sp(\varepsilon_1, \ldots, \varepsilon_l)| .$$

Proof. *(i)* Put $X = Q(l)^{\varepsilon_l} \ldots Q(1)^{\varepsilon_1}$ so that $|\text{inn } X| = |X/Z(X)| = q^{\lambda}$. The result then follows from Lemmas 4.2.1 and 4.2.7 and Theorems 4.2.2 and 4.2.6.

(ii) Put $X = Q(n_1, 1)Q(l)^{\varepsilon_l} \ldots Q(1)^{\varepsilon_1}$ so that $|\text{inn } X| = q^{2+\lambda}$. Substituting $\alpha = 1$, $m = n_1\text{-}1$, $r_1 = 1$ in Theorem 4.2.6, we have

$$|QSp(\varepsilon_1, \ldots, \varepsilon_l)| = q^{1+\lambda}|Sp(\varepsilon_1, \ldots, \varepsilon_l)|$$

since $I_0 = \{i : 1 \leq i \leq l\}$ and so $s_i = 1$, $t_i = 0$, $i \in I_0$. Lemma 4.2.1 and Theorem 4.2.2 then gives
$|\text{lin aut } X| = |\text{inn } X|.|QSp(\varepsilon_1, \ldots, \varepsilon_l)|$.

(iii) Put $X = Q(n_1, n_1\text{-}1)Q(l)^{\varepsilon_l} \ldots Q(1)^{\varepsilon_1}$ so that $|\text{inn } X| = q^{2(n_1-1)+\lambda}$. Suppose $l < n_1\text{-}1$. With the notations of 4.2, we have $I_1 = \{i : 1 \leq i < n_1\text{-}1\}$ and so $s_i = 0$, $t_i = 2$, $i = 1, \ldots, l$. Hence

$$\sum_{i=1}^{l} (s_i+it_i)\varepsilon_i = 2 \sum_{i=1}^{l} i\varepsilon_i = \lambda + \mu .$$

Next suppose $l = n_1\text{-}1$. Then $I_1 = \{i : 1 \leq i < l\}$, $I_0 = \{l\}$ and so

$$s_l = 2l - 1 , \quad t_l = 0 , \quad s_i = 0 , \quad t_i = 2 , \quad i \in I_1 .$$

Hence $\sum_{i=1}^{l} (s_i+it_i)\varepsilon_i = 2 \sum_{i=1}^{l-1} i\varepsilon_i + (2l-1)\varepsilon_l = \lambda + \mu - \varepsilon_l$. In other words, $\sum_{i=1}^{l} (s_i+it_i)\varepsilon_i = \lambda + \mu - \varepsilon_l\delta_{l,n_1-1}$. Substituting the relevant values in Theorem 4.2.6 and using Lemma 4.2.1, Theorem 4.2.2, we get

the required result. //

5.2.8 LEMMA.

$$c_n\{Q(n_1, 0)Q(l)^{\varepsilon_l} \dots Q(1)^{\varepsilon_1}\} + c_n\{Q(n_1, 1)Q(l)^{\varepsilon_l} \dots Q(1)^{\varepsilon_1}\}$$
$$= q^{(n_1-l)n-1}(q^{n-\lambda}-1)c_n\{Q(l)^{\varepsilon_l} \dots Q(1)^{\varepsilon_1}\} .$$

Proof. Write $X_0 = Q(l)^{\varepsilon_l} \dots Q(1)^{\varepsilon_1}$, $X = Q(n_1, 0)Q(l)^{\varepsilon_l} \dots Q(1)^{\varepsilon_1}$, $Y = Q(n_1, 1)Q(l)^{\varepsilon_l} \dots Q(1)^{\varepsilon_1}$. By Lemma 5.2.1, $\deg X = \deg X_0$, $\deg Y = q \deg X_0$. From Lemma 5.2.6 we get

$$k_n(X) = q^{(n_1-l-1)n}(q^n-q^\lambda)k_n(X_0)$$

$$k_n(Y) = q^{(n_1-l-1)n}(q^n-q^{1+\lambda})(q^n-q^\lambda)k_n(X_0) .$$

And Lemma 5.2.7 gives

$$|\text{lin aut } X| = |\text{lin aut } X_0| , \quad |\text{lin aut } Y| = q^{3+\lambda}|\text{lin aut } X_0| .$$

Hence by the introductory remarks of this section, we obtain

$$c_n(X) = q^{(n_1-l-1)n}(q^n-q^\lambda)c_n(X_0) ,$$

$$c_n(Y) = q^{(n_1-l-1)n-\lambda-1}(q^n-q^{1+\lambda})(q^n-q^\lambda)c_n(X_0) .$$

Adding, we get the required expression. //

5.2.9 LEMMA. *Let* $\gamma = (3n_1-l-5)n - 3n_1 + 5 + 2\varepsilon_l\delta_{l,n_1-1}$. *Then*

$$c_n\{Q(n_1, n_1-1)Q(l)^{\varepsilon_l} \dots Q(1)^{\varepsilon_1}\} = q^\gamma\{q^{2(n-\lambda-\mu)} - (q+1)q^{n-\lambda-2\mu} + q^{1-2\mu}\} \times$$
$$\times c_n\{Q(l)^{\varepsilon_l} \dots Q(1)^{\varepsilon_1}\} .$$

Proof. Write $X_0 = Q(l)^{\varepsilon_l} \dots Q(1)^{\varepsilon_1}$, $X = Q(n_1, n_1-1)Q(l)^{\varepsilon_l} \dots Q(1)^{\varepsilon_1}$. By Lemma 5.2.1, $\deg X = q^{n_1-1} \deg X_0$, and Lemmas 5.2.6 and 5.2.7 give

$$k_n(X) = q^{(3n_1-l-5)n}(q^n-q^{l+\lambda})(q^n-q^{\lambda})k_n(X_0) ,$$

$$|\text{lin aut } X| = q^{5n_1+2\lambda+2\mu-7-2\varepsilon_l\delta_{l,n_1-1}}|\text{lin aut } X_0| .$$

Substituting into the formula $c_n(X) = (\deg X)^2 k_n(X)/|\text{lin aut } X|$ and rewriting, we get the required result. //

In the rest of this chapter we will use the following notation:

$$c_n(r, s, t) = q^{2n(s+2t)+r(r-1)-(s+t)(s+3t)-2s-3t} \times$$

$$\times \prod_{i=1}^{2(r+s+t)} (q^{n-i+1}-1) \prod_{i=1}^{r} (q^{2i}-1)^{-1} \prod_{i=1}^{s} (q^{2i}-1)^{-1} \prod_{i=1}^{t} (q^{2i}-1)^{-1} ,$$

$$r, s, t \geq 0 .$$

For given r, s, t , $n \mapsto c_n(r, s, t)$ defines a function on $N^+ \cup \{0\}$. As we will see in 5.3, the CREAM problem for the case under consideration reduces to a study of some properties of $c_n(r, s, t)$. But first an essential observation.

5.2.10 LEMMA.

(i) For $r \geq 1$, $c_n(Q(1)^r) = q^n c_n(r, 0, 0)$.

(ii) For $r \geq 0$, $s \geq 1$, $c_n(Q(1)^r Q(2)^s) = q^{2n} c_n(r, s, 0)$.

(iii) For $r, s \geq 0$, $t \geq 1$,

$$c_n(Q(1)^r Q(2)^s Q(3)^t) = q^{3n} c_n(r, s, t) .$$

Proof. Write $X = Q(l)^{\varepsilon_l} \ldots Q(1)^{\varepsilon_1}$, $l \geq 1$. Then by Lemma 5.2.1, $\deg X = q^{\frac{1}{2}\lambda}$ where $\lambda = 2 \sum_{i=1}^{l} \varepsilon_i$, while by Corollary 5.2.5, Lemma 5.2.6 *(i)*,

$$k_n(X) = q^{(l+\mu)n+\frac{1}{2}\lambda(\lambda-1)} \prod_{i=1}^{\lambda} (q^{n-i+1}-1) .$$

By Lemma 5.2.7 *(i)*, $|\text{lin aut } X| = q^{\lambda}|Sp(\varepsilon_1, \ldots, \varepsilon_l)|$, where

$|Sp(\varepsilon_1, \ldots, \varepsilon_l)|$ is given in Theorem 4.2.6. Substituting the appropriate values in the formula $c_n(X) = (\deg X)^2 k_n(X)/|\text{lin aut } X|$, we get the required expressions. //

5.3 Some positive results on the CREAM problem

In considering the CREAM problem for subvarieties of $\underline{\underline{A}}_r \underline{\underline{W}}$ where $\underline{\underline{W}} = \underline{\underline{N}}_2 \wedge \underline{\underline{B}}_s$ with r, s coprime, we only need to consider those subvarieties satisfying $\underline{\underline{W}} \leq \underline{\underline{V}} \leq \underline{\underline{A}}_r \underline{\underline{W}}$. For if $\underline{\underline{V}} \not\geq \underline{\underline{W}}$, then put $\underline{\underline{U}}_1 = \underline{\underline{V}} \vee \underline{\underline{W}}$, $\underline{\underline{U}}_2 = \underline{\underline{V}} \wedge \underline{\underline{W}}$ so that $\underline{\underline{W}} \leq \underline{\underline{U}}_1 \leq \underline{\underline{A}}_r \underline{\underline{W}}$. By §§1.1, 1.3, Higman [15], a nilpotent variety is CREAM and hence $\underline{\underline{U}}_2$ is CREAM. By Lemma 1.2.3,

$$|F_n(\underline{\underline{V}})| = |F_n(\underline{\underline{U}}_1)| . |F_n(\underline{\underline{U}}_2)| . |F_n(\underline{\underline{W}})|^{-1} .$$

Moreover it is clear from Lemma 5.3.4 that $n \mapsto |F_n(\underline{\underline{W}})|^{-1}$, $n \in N^+$, is the restriction of a CREAM function. Hence the problem reduces to the question of whether $\underline{\underline{U}}_1$ is CREAM, by virtue of Lemma 1.1.1.

The CREAM problem for subvarieties satisfying $\underline{\underline{W}} \leq \underline{\underline{V}} \leq \underline{\underline{A}}_r \underline{\underline{W}}$ can again be reduced to the case when r is a prime power. For suppose $r = r_1 r_2$ with r_1 coprime to r_2. Then $\underline{\underline{V}} = \underline{\underline{V}}_1 \vee \underline{\underline{V}}_2$ where $\underline{\underline{V}}_i = \underline{\underline{V}} \wedge \underline{\underline{A}}_{r_i} \underline{\underline{W}}$, $i = 1, 2$, and $\underline{\underline{V}}_1 \wedge \underline{\underline{V}}_2 = \underline{\underline{W}}$. Clearly $\underline{\underline{W}} \leq \underline{\underline{V}}_i \leq \underline{\underline{A}}_{r_i} \underline{\underline{W}}$, $i = 1, 2$. As before,

$$|F_n(\underline{\underline{V}})| = |F_n(\underline{\underline{V}}_1)| . |F_n(\underline{\underline{V}}_2)| . |F_n(\underline{\underline{W}})|^{-1} ,$$

and it only remains to see whether $\underline{\underline{V}}$ is CREAM for $i = 1, 2$. Furthermore Higman [15] has shown that this CREAM problem for the case when $r = p^i$, where p is a prime, can be reduced to the case when $r = p$. Finally since each irreducible linear group in $\underline{\underline{W}}$ is nilpotent and hence is the direct product of its Sylow subgroups, we can reduce the problem further to the case when s itself is a prime power.

With the above remarks in mind, we easily deduce Theorem 5.3.1 from Theorem 5.3.2.

5.3.1 THEOREM. *Let r, s be positive coprime integers where s is an odd integer not divisible by q^4 for any prime q. Then the subvarieties of $\underline{\underline{A}}_r(\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_s)$ are* CREAM .

5.3.2 THEOREM. *Let p, q be distinct primes with q odd. Then the subvarieties of $\underline{\underline{A}}_p(\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_{q^3})$ are* CREAM .

In view of the concluding remarks of 1.2, Theorem 5.3.2 itself follows immediately from the next theorem. We will use the notation $\underline{\underline{Q}}_i$ and the description of the derived classes of a closed class $\underline{\underline{X}} \leq \underline{\underline{Q}}_3$ in 5.1. To simplify the terminology, we will say that a non-empty (not necessarily closed) class $\underline{\underline{S}}$ of irreducible linear groups is CREAM if $n \mapsto c_n(\underline{\underline{S}})$, $n \in N^+$, is the restriction of a CREAM function to N^+.

5.3.3 THEOREM. *Every non-empty closed class $\underline{\underline{X}} \leq \underline{\underline{Q}}_3$ is* CREAM .

Proof. (i) $\underline{\underline{X}} \leq \underline{\underline{Q}}_1$. If $\underline{\underline{X}} = \underline{\underline{Q}}_1$, then $\underline{\underline{X}}$ is CREAM by Lemma 5.3.5. If $\underline{\underline{X}} \neq \underline{\underline{Q}}_1$, then $\underline{\underline{X}}$ is clearly finite and so is CREAM by Theorem 1.2.12.

(ii) $\underline{\underline{X}} \leq \underline{\underline{Q}}_2$, $\underline{\underline{X}} \not\leq \underline{\underline{Q}}_1$. Suppose $\underline{\underline{S}}_0$, $\underline{\underline{S}}_1$, $\underline{\underline{S}}^j$, $j \geq 0$, are the derived classes of $\underline{\underline{X}}$. We may assume ν = index of $\underline{\underline{X}} < \infty$. Otherwise $\underline{\underline{X}} = \underline{\underline{Q}}_2$ by Theorem 3.3.3 and $\underline{\underline{X}}$ is then CREAM by Lemma 5.3.5. Also $\underline{\underline{S}}^0 \leq \underline{\underline{Q}}_1$ is closed and hence is CREAM by (i).

If $\underline{\underline{S}}_0$ has rank 0, then so do $\underline{\underline{S}}_1$, $\underline{\underline{S}}^j$, $j > 0$, by Lemma 5.1.1. Hence $\underline{\underline{S}}_0 \cup \underline{\underline{S}}_1 \cup \underline{\underline{S}}^1 \cup \ldots \cup \underline{\underline{S}}^\nu$ is finite and CREAM, and so $\underline{\underline{X}}$ is CREAM by Lemma 5.1.2.

If $\underline{\underline{S}}_0$ has rank 1, then $\underline{\underline{S}}^0 \cup \underline{\underline{S}}_0 \cup \underline{\underline{S}}_1$ is CREAM by Lemma 5.1.5 and Theorem 1.2.4. If $\underline{\underline{S}}^j$ has rank 0 for $j = 1, \ldots, \nu$, then $\bigcup_{j=1}^{\nu} \underline{\underline{S}}^j$ is finite and hence CREAM. So suppose $\underline{\underline{S}}^j$ has rank 1

for some $1 \le j \le \nu$. Let $1 \le \lambda \le \nu$ be the largest integer for which $\underline{\underline{S}}^{\lambda}$ has rank 1. Then

$$\underline{\underline{S}}^{j} = \{Q(2)^{j}Q(1)^{r} : r = 0, 1, \ldots\}, \quad 1 \le j \le \lambda,$$

and so is CREAM by Lemma 5.3.12. Since $\bigcup_{j=\lambda+1}^{\nu} \mathcal{S}^{j}$ is finite (or empty), it follows that $\bigcup_{j=1}^{\nu} \mathcal{S}^{j}$ is CREAM. Hence $\underline{\underline{X}}$ is CREAM.

(iii) $\underline{\underline{X}} \le \underline{\underline{Q}}_3$, $\underline{\underline{X}} \not\le \underline{\underline{Q}}_2$. Suppose $\underline{\underline{S}}_0, \underline{\underline{S}}_1, \underline{\underline{S}}_2, \underline{\underline{S}}^{j}$, $j \ge 0$, are the derived classes of $\underline{\underline{X}}$. Again we may assume ν = index of $\underline{\underline{X}} < \infty$. Since $\underline{\underline{S}}^{0} \le \underline{\underline{Q}}_2$ is closed, $\underline{\underline{S}}^{0}$ is CREAM by (i) and (ii).

If $\underline{\underline{S}}_0$ has rank 0, then so do $\underline{\underline{S}}_1, \underline{\underline{S}}_2, \underline{\underline{S}}^{j}$, $j > 0$, by Lemma 5.1.1. Hence by Lemma 5.1.2, $\underline{\underline{X}}$ is the disjoint union of $\underline{\underline{S}}^{0}$ and a finite set and hence is CREAM.

If $\underline{\underline{S}}_0$ has rank 1, then so has $\underline{\underline{S}}_1$ by Lemma 5.1.1. We have from Lemma 5.1.4

$$\underline{\underline{S}}_0 = \bigcup_{s=0}^{\sigma_0} \left\{Q(3, 0)Q(2)^{s}Q(1)^{r} : r = 0, 1, \ldots, \rho_{0s}\right\},$$

$$\underline{\underline{S}}_1 = \bigcup_{s=0}^{\sigma_1} \left\{Q(3, 1)Q(2)^{s}Q(1)^{r} : r = 0, 1, \ldots, \rho_{1s}\right\},$$

where $\sigma_0, \sigma_1 < \infty$. Clearly $\rho_{0s} = \infty$ if and only if $\rho_{1s} = \infty$. Let $0 \le \tau \le \max\{\sigma_0, \sigma_1\}$ be the largest integer for which $\rho_{0\tau} = \infty$. Then

$$\underline{\underline{S}}_0 = \bigcup_{s=0}^{\tau} \{Q(3, 0)Q(2)^{s}Q(1)^{r} : r = 0, 1, \ldots\} \cup \underline{\underline{S}}'_0,$$

$$\underline{\underline{S}}_1 = \bigcup_{s=0}^{\tau} \{Q(3, 1)Q(2)^{s}Q(1)^{r} : r = 0, 1, \ldots\} \cup \underline{\underline{S}}'_1,$$

where the unions are disjoint, and $\underline{\underline{S}}'_0, \underline{\underline{S}}'_1$ are finite (or empty). By Lemma 5.3.14,

$$\{Q(3, 0)Q(2)^{s}Q(1)^{r}, Q(3, 1)Q(2)^{s}Q(1)^{r} : r = 0, 1, \ldots\}$$

is CREAM for every $0 \le s \le \tau$. Hence $\underline{\underline{S}}_0 \cup \underline{\underline{S}}_1$ is CREAM. Without

loss of generality, suppose rank of $\underline{\underline{S}}_2$ is 1, in which case by Lemma 5.1.4,

$$\underline{\underline{S}}_2 = \bigcup_{s=0}^{\sigma_2} \left\{ Q(3, 2)Q(2)^s Q(1)^r : r = 0, 1, \ldots, \rho_{2s} \right\}, \quad \sigma_2 < \infty .$$

Let $0 \leq \tau' \leq \sigma_2$ be the largest integer for which $\rho_{2\tau'} = \infty$. Then

$$\underline{\underline{S}}_2 = \bigcup_{s=0}^{\tau'} \{ Q(3, 2)Q(2)^s Q(1)^r : r = 0, 1, \ldots \} \cup \underline{\underline{S}}'_2$$

where the union is disjoint and $\underline{\underline{S}}'_2$ is finite (or empty). By Lemma 5.3.15, each of the infinite class in the above union is CREAM. Hence $\underline{\underline{S}}_2$ is CREAM, and so $\bigcup_{i=0}^{2} \underline{\underline{S}}_i$ is CREAM.

If $\underline{\underline{S}}_0$ has rank 2, then by Lemma 5.1.6 and Theorem 1.2.4, $\underline{\underline{S}}^0 \cup \left(\bigcup_{i=0}^{2} \underline{\underline{S}}_i \right)$ is CREAM. Thus it remains to prove that $\underline{\underline{S}}^j$, $1 \leq j \leq \nu$, is CREAM for $\underline{\underline{S}}^j$ of rank 1 or 2. Firstly if $\underline{\underline{S}}^j$ has rank 1, then from Lemma 5.1.4,

$$\underline{\underline{S}}^j = \bigcup_{s=0}^{\mu_j} \left\{ Q(3)^j Q(2)^s Q(1)^r : r = 0, 1, \ldots, \lambda_{js} \right\}, \quad \mu_j < \infty .$$

Let $0 \leq \delta_j \leq \mu_j$ be the largest integer for which $\lambda_{j\delta_j} = \infty$. Then

$$\underline{\underline{S}}^j = \bigcup_{s=0}^{\delta_j} \{ Q(3)^j Q(2)^s Q(1)^r : r = 0, 1, \ldots \} \cup \underline{\underline{T}}^j$$

where the union is disjoint and $\underline{\underline{T}}^j$ is finite (or empty). Each of the infinite class in this union is CREAM by Lemma 5.3.13. Hence $\underline{\underline{S}}^j$ is CREAM.

Finally if $\underline{\underline{S}}^j$ has rank 2, then by Lemma 5.1.4,

$$\underline{\underline{S}}^j = \{ Q(3)^j Q(2)^s Q(1)^r : r, \quad = 0, 1, \ldots \}$$

and so is CREAM by Lemma 5.3.16. //

We now prove the lemmas used in the above discussion and in the proofs of the above theorems of this section.

5.3.4 LEMMA. $|F_n(\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_s)| = s^{\frac{1}{2}n(n+1)}$.

Proof. Write

$$G_n = F_n(\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_s) = \langle x_1, \ldots, x_n : x_i^s = [x_i, x_j]^s = [x_i, x_j, x_k] = 1 , \quad i \neq j , \ i, j, k = 1, \ldots, n \rangle .$$

Since G_n is of class 2 , $[x_i x_j, x_k] = [x_i, x_k][x_j, x_k]$ and so

$$G_n' = \langle [x_i, x_j] : i, j = 1, \ldots, n \rangle .$$

Now G_n' is a direct product of $\frac{1}{2}n(n-1)$ s-cycles, and evidently G_n/G_n' is a direct product of n s-cycles. Hence

$$|G_n| = |G_n/G_n'| . |G_n'| = s^{\frac{1}{2}n(n+1)} . \qquad //$$

5.3.5 LEMMA. $\underline{\underline{Q}}_i$ *is* CREAM *for* $i \geq 1$.

Proof. From Lemma 1.2.8, we have $c_n(\underline{\underline{Q}}_i) = |F_n(\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_{q^i})|$, and so by Lemma 5.3.4, $n \mapsto c_n(\underline{\underline{Q}}_i)$, $n \in N^+$, is evidently the restriction of a CREAM function. //

We will find it convenient to consider functions of $n \in N^+ \cup \{0\}$ in the following lemmas. For brevity we will say that $f(n)$ is CREAM if $n \mapsto f(n)$, $n \in N^+ \cup \{0\}$, is the restriction of a CREAM function to $N^+ \cup \{0\}$. Note also that in each of the following (apparently) infinite sums there are only finitely many terms for each fixed $n \in N^+ \cup \{0\}$ so that these sums are finite.

5.3.6 LEMMA. $\sum_{r=1}^{\infty} c_n(r, 0, 0)$ *is* CREAM .

Proof. For $n > 0$, we have

$$c_n(\underline{\underline{Q}}_1) = c_n(1) + c_n\{Q(1, 0)\} + \sum_{r=1}^{\infty} c_n\{Q(1)^r\}$$

$$= 1 + (q^n - 1) + q^n \sum_{r=1}^{\infty} c_n(r, 0, 0) ,$$

using Lemma 5.2.10 *(i)*. Hence from the proof of Lemma 5.3.5, we have

$$\sum_{r=1}^{\infty} c_n(r, 0, 0) = q^{\frac{1}{2}n(n-1)} - 1 , \quad n > 0 .$$

Clearly $c_0(r, 0, 0) = 0$ for $r > 0$. So the above relation holds for $n \geq 0$. Hence $\sum_{r=1}^{\infty} c_n(r, 0, 0)$ is evidently CREAM. //

As a corollary we have the polynomial identity

5.3.7 COROLLARY.

$$\sum_{r=0}^{[\frac{1}{2}n]} x^{r(r-1)} \prod_{i=1}^{2r} (x^{n-i+1}-1) \prod_{i=1}^{r} (x^{2i}-1)^{-1} = x^{\frac{1}{2}n(n-1)} .$$

5.3.8 LEMMA. $\sum_{r=0}^{\infty} \sum_{s=1}^{\infty} c_n(r, s, 0)$ *is* CREAM.

Proof. From Lemma 5.1.5, we have

$$\underline{\underline{Q}}_2 = \underline{\underline{Y}} \cup \{Q(1)^r Q(2)^s : r = 0, 1, \ldots , \ s = 1, 2, \ldots\} ,$$

where $\underline{\underline{Y}}$ is the class of all irreducible linear groups in $\underline{\underline{A}}_{q^2} \vee (\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_q) = \underline{\underline{W}}_0$ say. From the proof of Theorem 1.2.4, we deduce that

$$c_n(\underline{\underline{Y}}) = |F_n(\underline{\underline{W}}_0)| .$$

Since $\underline{\underline{A}}_{q^2} \wedge (\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_q) = \underline{\underline{A}}_q$, Lemma 1.2.3 then gives

$$|F_n(\underline{\underline{A}}_q)| . |F_n(\underline{\underline{W}}_0)| = |F_n(\underline{\underline{A}}_{q^2})| . |F_n(\underline{\underline{N}}_2 \wedge \underline{\underline{B}}_q)| .$$

Hence by Lemmas 5.2.10*(ii)* and 5.3.4 and the proof of Lemma 5.3.5,

$$\sum_{r=0}^{\infty} \sum_{s=1}^{\infty} c_n(r, s, 0) = q^{-2n}\{c_n(\underline{\underline{Q}}_2) - c_n(\underline{\underline{Y}})\}$$

$$= q^{n(n-1)} - q^{\frac{1}{2}n(n-1)} , \quad n > 0 .$$

Plainly the above relation is also true for $n = 0$. Hence the result. //

5.3.9 LEMMA. $\sum_{r=1}^{\infty} q^{-2kr} c_n(r, s, 0)$ *is* CREAM *for* $s, k \geq 0$.

Proof. Write $b_{n,k}(r, s, 0) = q^{-2kr} c_n(r, s, 0)$, $s, k \geq 0$, and $f_k(n) = \sum_{r=1}^{\infty} b_{n,k}(r, 0, 0)$. Since $c_0(r, 0, 0) = c_1(r, 0, 0)$, $r > 0$, $f_k(0) = f_k(1) = 0$, $k \geq 0$. We use induction on k to show that $f_k(n)$ is CREAM for $k \geq 0$. Clearly $f_0(n)$ is CREAM by Lemma 5.3.6. Suppose now $k > 0$ and $f_{k-1}(n)$ is CREAM . We have

$$b_{n,k}(r, 0, 0) = q^{r(r-2k-1)} \prod_{i=1}^{2r} (q^{n-i+1}-1) \prod_{i=1}^{r} (q^{2i}-1)^{-1} ,$$

so that for $n \geq 2$, $r \geq 1$,

$$(q^{2r}-1) b_{n,k}(r, 0, 0) = q^{-2k}(q^n-1)(q^{n-1}-1) b_{n-2,k-1}(r-1, 0, 0) ,$$

or

$$b_{n,k}(r, 0, 0) = b_{n,k-1}(r, 0, 0) - q^{-2k}(q^n-1)(q^{n-1}-1) b_{n-2,k-1}(r-1, 0, 0) .$$

Summing from $r = 1$ to $r = \infty$, we have for $n \geq 2$,

$$f_k(n) = f_{k-1}(n) - f(n)\{1+f_{k-1}(n-2)\} ,$$

where f is the CREAM function $x \mapsto q^{-2k}(q^x-1)(q^{x-1}-1)$, $x \in \mathbb{R}$. By hypothesis, there is a CREAM function $\alpha : \mathbb{R} \to \mathbb{R}$ such that

$$\alpha(n) = f_{k-1}(n) , \quad n \in \mathbb{N}^+ \cup \{0\} .$$

Let $\beta = j - 2$ where j is the identity function on $\mathbb{R}$ so that $\gamma = \alpha \circ \beta$ is a CREAM function by Lemma 1.1.3, and

$$\gamma(n) = f_{k-1}(n-2) , \quad n = 2, 3, \ldots .$$

Define the function $\lambda : x \mapsto \alpha(x) - f(x)\{1+\gamma(x)\}$, $x \in \mathbb{R}$. By Lemmas 1.1.1 and 1.1.3, λ is a CREAM function. It is clear that since γ is a CREAM function, $\gamma(0)$ and $\gamma(1)$ are finite so that $\lambda(0) = \lambda(1) = 0$. Hence $\lambda(n) = f_k(n)$, $n \in \mathbb{N}^+ \cup \{0\}$, and so $f_k(n)$ is CREAM .

For a fixed $k \geq 0$, write

$$g_s(n) = \sum_{r=1}^{\infty} b_{n,k}(r, s, 0) , \quad s \geq 0 .$$

Since $c_0(r, s, 0) = c_1(r, s, 0) = 0$ for $r+s > 0$, and $c_2(r, s, 0) = 0$ for $r, s > 0$, it follows that $g_s(0) = g_s(1) = 0$ for $s \geq 0$, and $g_s(2) = 0$ for $s > 0$. We use induction on s to show that $g_s(n)$ is CREAM for $s \geq 0$. Clearly $g_0(n) = f_k(n)$ is CREAM. So suppose $s > 0$ and $g_{s-1}(n)$ is CREAM. It can be checked that for $r, s \geq 1$, $n \geq 2$,

$$b_{n,k}(r, s, 0) = q^{2n-2s-5}(q^n-1)(q^{n-1}-1)(q^{2s}-1)^{-1}b_{n-2,k}(r, s-1, 0) .$$

Hence for $n \geq 2$, $g_s(n) = g(n)g_{s-1}(n-2)$, where g is the CREAM function $x \mapsto q^{2x-2s-5}(q^x-1)(q^{x-1}-1)(q^{2s}-1)^{-1}$, $x \in \mathbb{R}$. By hypothesis, there is a CREAM function $\delta : \mathbb{R} \to \mathbb{R}$ such that

$$\delta(n) = g_{s-1}(n) , \quad n \in N^+ \cup \{0\} .$$

Put $\varepsilon = \delta \circ \beta$ where $\beta = j - 2$. Then ε is a CREAM function and

$$\varepsilon(n) = g_{s-1}(n-2) , \quad n = 2, 3, \ldots .$$

Moreover $\varepsilon(0)$, $\varepsilon(1)$ are finite, so that $\tau(0) = \tau(1) = 0$, where τ is the CREAM function $x \mapsto g(x)\varepsilon(x)$, $x \in \mathbb{R}$. Evidently

$$\tau(n) = g_s(n) , \quad n \in N^+ \cup \{0\} .$$

Hence $g_s(n)$ is CREAM. //

5.3.10 LEMMA. $\sum_{r=1}^{\infty} c_n(r, s, t)$ *is* CREAM *for* $s, t \geq 0$.

Proof. For a fixed $s \geq 0$, write $h_t(n) = \sum_{r=1}^{\infty} c_n(r, s, t)$, $t \geq 0$. Since the proof by induction on t is similar to the second part of the proof of Lemma 5.3.9, we will omit the details. We merely note that $h_0(n)$ is CREAM by the preceding lemma and that $h_t(0) = h_t(1) = 0$ for $t \geq 0$. Moreover it can be checked that for $r, s \geq 0$, $t \geq 1$, $n \geq 2$,

$$c_n(r, s, t) = c(n)c_{n-2}(r, s, t-1) ,$$

where $c(n) = q^{4n+2t-8}(q^n-1)(q^{n-1}-1)(q^{2t}-1)^{-1}$, so that

$$h_t(n) = c(n)h_{t-1}(n-2) \ , \quad t > 0 \ , \quad n \geq 2 \ . \qquad //$$

5.3.11 LEMMA. $\sum_{r=0}^{\infty} \sum_{s=0}^{\infty} c_n(r, s, t)$ *is* CREAM *for* $t \geq 0$.

Proof. Write $u_t(n) = \sum_{r=0}^{\infty} c_n(r, 0, t) + \sum_{r=0}^{\infty} \sum_{s=1}^{\infty} c_n(r, s, t)$, $t \geq 0$. It is clear that $u_0(n)$ is CREAM by Lemmas 5.3.6 and 5.3.8. Since

$$c_0(r, s, t) = c_1(r, s, t) = 0 \quad \text{if} \quad r+s+t > 0 \ ,$$

it follows that $u_t(0) = u_t(1) = 0$ for $t > 0$. From the proof of Lemma 5.3.10 and using its notations, we have

$$u_t(n) = c(n)u_{t-1}(n-2) \ , \quad t > 0 \ , \quad n \geq 2 \ .$$

The proof by induction on t then follows as in the second part of the proof of Lemma 5.3.9. //

We will now relate the above CREAM results to the classes of irreducible linear groups in $\underline{\underline{Q}}_3$.

5.3.12 LEMMA. $\{Q(2)^s Q(1)^r : r = 0, 1, \ldots\}$ *is* CREAM *for* $s > 0$.

Proof. For a fixed $s > 0$, we have to show that

$$n \mapsto \sum_{r=0}^{\infty} c_n\{Q(2)^s Q(1)^r\} \ , \quad n \in N^+ \ ,$$

is the restriction of a CREAM function to N^+ . Since by Lemma 5.2.10 *(ii)*,

$$c_n\{Q(2)^s Q(1)^r\} = q^{2n} c_n(r, s, 0) \ ,$$

it is enough to show that $n \mapsto \sum_{r=0}^{\infty} c_n(r, s, 0)$, $n \in N^+$, is the restriction of a CREAM function. Now clearly $n \mapsto c_n(0, s, 0)$, $n \in N^+$, is the restriction of a CREAM function. So also is

$$n \mapsto \sum_{r=1}^{\infty} c_n(r, s, 0) \ , \quad n \in N^+ \ ,$$

by Lemma 5.3.9 (with $k = 0$). Hence the required result follows from

$$\sum_{r=0}^{\infty} c_n(r, s, 0) = c_n(0, s, 0) + \sum_{r=1}^{\infty} c_n(r, s, 0) . \qquad //$$

5.3.13 LEMMA. $\{Q(3)^t Q(2)^s Q(1)^r : r = 0, 1, \ldots\}$ *is* CREAM *for* $s \geq t$, $t > 0$.

Proof. It is clear that for fixed $s \geq 0$, $t > 0$, $n \mapsto c_n(0, s, t)$, $n \in N^+$, is the restriction of a CREAM function. So also is $n \mapsto \sum_{r=1}^{\infty} c_n(r, s, t)$, $n \in N^+$, by Lemma 5.3.10. Since by Lemma 5.2.10 *(iii)*,

$$\sum_{r=0}^{\infty} c_n\{Q(3)^t Q(2)^s Q(1)^r\} = q^{3n}\left\{c_n(0, s, t) + \sum_{r=1}^{\infty} c_n(r, s, t)\right\}, \quad n \in N^+,$$

the result follows immediately. //

5.3.14 LEMMA. $\{Q(3, 0)Q(2)^s Q(1)^r, Q(3, 1)Q(2)^s Q(1)^r : r = 0, 1, \ldots\}$ *is* CREAM *for* $s \geq 0$.

Proof. By Theorem 1.2.12, it is sufficient to show that

$$\{Q(3, 0)Q(2)^s Q(1)^r, Q(3, 1)Q(2)^s Q(1)^r : r = 1, 2, \ldots\}$$

is CREAM. Considering the cases $s = 0$ and $s > 0$ separately, we have by Lemmas 5.2.8 and 5.2.10,

$$\sum_{r=1}^{\infty} \left\{c_n\{Q(3, 0)Q(2)^s Q(1)^r\} + c_n\{Q(3, 1)Q(2)^s Q(1)^r\}\right\}$$

$$= q^{4n-2s-1} \sum_{r=1}^{\infty} q^{-2r} c_n(r, s, 0) - q^{3n-1} \sum_{r=1}^{\infty} c_n(r, s, 0), \quad n \in N^+ .$$

Hence the result follows from Lemma 5.3.9. //

5.3.15 LEMMA. $\{Q(3, 2)Q(2)^s Q(1)^r : r = 0, 1, \ldots\}$ *is* CREAM *for* $s \geq 0$.

Proof. Again by Theorem 1.2.12, it is enough to show that

$$\{Q(3, 2)Q(2)^s Q(1)^r : r = 1, 2, \ldots\}$$

is CREAM. Considering the cases $s = 0$ and $s > 0$ separately, we

have by Lemmas 5.2.9 and 5.2.10,

$$\sum_{r=1}^{\infty} c_n\{Q(3,\ 2)Q(2)^s Q(1)^r\} = q^{6n-6s-4} \sum_{r=1}^{\infty} q^{-4r}\, c_n(r,\ s,\ 0)$$

$$-(q+1)q^{5n-4s-4} \sum_{r=1}^{\infty} q^{-2r} c_n(r,\ s,\ 0)$$

$$+\ q^{4n-2s-3} \sum_{r=1}^{\infty} c_n(r,\ s,\ 0)\ ,\quad n \in N^+\ .$$

The result then follows from Lemma 5.3.9. //

5.3.16 LEMMA. $\{Q(3)^t Q(2)^s Q(1)^r : r,\ s = 0,\ 1,\ \ldots\}$ *is* CREAM *for* $t > 0$.

Proof. By Lemma 5.2.10 *(iii)*,

$$\sum_{r=0}^{\infty} \sum_{s=0}^{\infty} c_n\{Q(3)^t Q(2)^s Q(1)^r\} = q^{3n} \sum_{r=0}^{\infty} \sum_{s=0}^{\infty} c_n(r,\ s,\ t)\ ,\quad n \in N^+\ .$$

Hence the result follows from Lemma 5.3.11. //

5.4 A non-CREAM class which is not closed

In this section we show that if $\underline{\underline{S}} = \{Q(4,\ 0)Q(1)^r : r = 1,\ 2,\ \ldots\}$, then $n \mapsto c_n(\underline{\underline{S}})$, $n \in N^+$, is not the restriction of a CREAM function to N^+ .

First we borrow a definition and a theorem of Hardy [11]. An *L*-function (or *logarithmico-exponential function*) is defined as a real one-valued function defined, for all values of x greater than some definite value, by a finite combination of the ordinary algebraic symbols (namely, +, -, ×, ÷, $\sqrt[n]{}$) and the functional symbols log(...) and $e^{(\ldots)}$, operating on the variable x and on real constants.

5.4.1 THEOREM (Hardy [11]). *Any L-function is ultimately continuous, of constant sign, and monotonic and tends, as* $x \to \infty$, *to infinity, or to zero or to some definite limit.*

The next lemma is immediate from the definitions.

5.4.2 LEMMA. *A* CREAM *function is an L-function.*

Proof. This is evident from the fact that for each $b \in Q^+$ and every CREAM function $f : \mathbb{R} \to \mathbb{R}$, $b^{f(x)} = e^{f(x)\log b}$, $x \in \mathbb{R}$. //

A consequence of Lemma 5.4.2 above and Lemma 5.4.6 below is the following

5.4.3 THEOREM. *Let* $\underline{\underline{S}} = \{Q(4, 0)Q(1)^r : r = 1, 2, \ldots\}$. *Then*

$$n \mapsto c_n(\underline{\underline{S}}), \quad n \in N^+,$$

is not the restriction to N^+ *of any* CREAM *function.*

Proof. From the proof of Lemma 5.2.8, we have

$$c_n\{Q(4, 0)Q(1)^r\} = q^{3n}(q^n - q^{2r})c_n\{Q(1)^r\}, \quad r > 0, \quad n \in N^+,$$

or using Lemma 5.2.10, we have for $n \in N^+$,

$$\sum_{r=0}^{\infty} q^{2r} c_n(r, 0, 0) = 1 + q^n \sum_{r=1}^{\infty} c_n(r, 0, 0) - q^{-3n} \sum_{r=1}^{\infty} c_n\{Q(4, 0)Q(1)^r\}.$$

Suppose the theorem is false. Then Lemma 5.3.6 implies that there is a CREAM function $f : \mathbb{R} \to \mathbb{R}$ such that

$$f(n) = \sum_{r=0}^{\infty} q^{2r} c_n(r, 0, 0), \quad n \in N^+.$$

By Lemma 5.4.2, f is an L-function. Plainly the function

$$x \mapsto f(x)q^{-\frac{1}{2}x(x+1)}, \quad x \in \mathbb{R},$$

is also an L-function, and so by Theorem 5.4.1, $f(x)q^{-\frac{1}{2}x(x+1)}$ tends to some definite limit as $x \to \infty$. It follows that $f(n)q^{-\frac{1}{2}n(n+1)}$ tends to a definite limit as $n \to \infty$, contradicting Lemma 5.4.6. Hence the theorem is proved. //

The remaining part of this section will be devoted to establishing Lemma 5.4.6. This is done via two lemmas. Henceforth we will write for every $n \in N^+$,

$$f(n) = \sum_{r=0}^{\infty} q^{2r} c_n(r, 0, 0),$$

$$g(n) = \prod_{i=1}^{n} (q^i - 1) ,$$

$$h(n) = q^{\frac{1}{2}n(n-1)} .$$

5.4.4 LEMMA. *For* $n \in N^+$,

$$\frac{f(n)}{g(n)} = \frac{h(n)}{g(n)} + \frac{h(n-2)}{g(n-2)} + \ldots + \frac{h(n-2j)}{g(n-2j)} + \ldots + \begin{cases} \dfrac{h(0)}{g(0)} & \text{if } n \text{ is even,} \\ \dfrac{h(1)}{g(1)} & \text{if } n \text{ is odd.} \end{cases}$$

Proof. Write

$$u_r(n) = q^{2r} c_n(r, 0, 0)$$

$$= q^{r(r+1)} \prod_{i=1}^{2r} (q^{n-i+1} - 1) \prod_{i=1}^{r} (q^{2i} - 1)^{-1} ,$$

for $r \geq 0$, $n \in N^+$. Then the following relation holds for $r > 0$, $n > 2$,

$$(q^n - 1)(q^{n-1} - 1) u_{r-1}(n-2) = (q^{2r} - 1) c_n(r, 0, 0) ,$$

or

$$u_r(n) = (q^n - 1)(q^{n-1} - 1) u_{r-1}(n-2) + c_n(r, 0, 0) .$$

This relation also holds for $r = 0$ if we set $u_{-1}(n) = 0$, $n \in N^+$. Hence summing from $r = 0$ to $r = \infty$, we have

$$f(n) = (q^n - 1)(q^{n-1} - 1) f(n-2) + h(n) , \quad n > 2 , \qquad (*)$$

since $\sum_{r=0}^{\infty} c_n(r, 0, 0) = h(n)$ by Corollary 5.3.7.

We now use induction on n . First it is easily checked that $f(1) = 1$, $f(2) = q^2(q-1) + 1$, so that the lemma is true for $n = 1$ and 2 . Suppose $n > 1$ is odd and that

$$\frac{f(n-2)}{g(n-2)} = \frac{h(n-2)}{g(n-2)} + \frac{h(n-4)}{g(n-4)} + \ldots + \frac{h(1)}{g(1)} .$$

Clearly $n > 2$ and the recurrence relation (*) then gives

$$\frac{f(n)}{g(n)} = \frac{f(n-2)}{g(n-2)} + \frac{h(n)}{g(n)} = \frac{h(n)}{g(n)} + \frac{h(n-2)}{g(n-2)} + \ldots + \frac{h(1)}{g(1)} .$$

Similarly for n even. //

The next result is an expansion due to Euler and is proved as in Bellman [2].

5.4.5 LEMMA. *For* $|x| < 1$, $|t| \leq 1$,

$$\prod_{i=1}^{\infty} (1-x^i t)^{-1} = \sum_{n=0}^{\infty} x^n t^n \prod_{i=1}^{n} (1-x^i)^{-1} .$$

Proof. By well-known results in analysis (see, for instance, Knopp, [17]), the infinite product is convergent and non-zero. Moreover each factor may be expanded as an infinite series

$$(1-x^i t)^{-1} = 1 + x^i t + (x^i t)^2 + \ldots , \quad i = 1, 2, \ldots ,$$

each of which is absolutely convergent and hence we can multiply them together and arrange the terms in any manner. Write

$$f(x, t) = \prod_{i=1}^{\infty} (1-x^i t)^{-1} .$$

Then $f(x, tx) = (1-xt)f(x, t)$. Let $f(x, t) = \sum_{n=0}^{\infty} a_n(x)t^n$. Substituting into the above functional equation and equating the coefficients of t^n , we have $a_n(x)x^n = a_n(x) - xa_{n-1}(x)$, $a_0(x) = 1$. Hence

$$a_n(x) = x^n \prod_{i=1}^{n} (1-x^i)^{-1} , \quad n \geq 0 . \qquad //$$

We can now prove

5.4.6 LEMMA. *The function* $n \mapsto f(n)q^{-\frac{1}{2}n(n+1)}$, $n \in N^+$, *does not tend to any limit as* $n \to \infty$.

Proof. We can write

$$f(n)/g(n) = f(n)q^{-\frac{1}{2}n(n+1)} \prod_{i=1}^{n} (1-y^i)^{-1} , \quad n \in N^+ ,$$

where $y = \frac{1}{q} < 1$. Suppose $f(n)q^{-\frac{1}{2}n(n+1)}$ tends to a definite limit as $n \to \infty$. Then since $\prod_{i=1}^{\infty} (1-y^i)$ is convergent and non-zero,

$f(n)/g(n)$ must tend to a definite limit as $n \to \infty$. Writing

$$h(n)/g(n) = y^n \prod_{i=1}^{n} (1-y^i)^{-1} ,$$

we have from Lemma 5.4.4,

$$f(2n)/g(2n) = \sum_{r=0}^{n} y^{2r} \prod_{i=1}^{2r} (1-y^i)^{-1} ,$$

$$f(2n+1)/g(2n+1) = \sum_{r=0}^{n} y^{2r+1} \prod_{i=1}^{2r+1} (1-y^i)^{-1} .$$

As $n \to \infty$, the two infinite series obtained are convergent by the ratio test, and hence $\lim_{n\to\infty} f(n)/g(n)$ is finite. Therefore

$$\begin{aligned} 0 &= \lim_{n\to\infty} f(2n)/g(2n) - \lim_{n\to\infty} f(2n+1)/g(2n+1) \\ &= \sum_{n=0}^{\infty} (-1)^n y^n \prod_{i=1}^{n} (1-y^i)^{-1} \\ &= \prod_{i=1}^{\infty} (1+y^i)^{-1} , \end{aligned}$$

by Lemma 5.4.5. This is a contradiction. //

REFERENCES

[1] E. Artin, *Geometric Algebra* (Interscience, New York, 1957).

[2] Richard Bellman, *A brief introduction to theta functions* (Holt, Rinehart and Winston, New York, 1961).

[3] J.M. Brady, "Just-non-Cross varieties of groups", Ph.D. thesis, Australian National University, 1970.

[4] J.M. Brady, R.A. Bryce and J. Cossey, "On certain abelian-by-nilpotent varieties", *Bull. Austral. Math. Soc.* 1 (1969), 403-416.

[5] John Cook, "Some varieties of groups", Ph.D. thesis, Balliol College, Oxford University, 1970.

[6] Charles W. Curtis and Irving Reiner, *Representation theory of finite groups and associative algebras* (Interscience, New York, 1966).

[7] Wolfgang Gaschütz, "Über modulare Darstellungen endlicher Gruppen, die von freien Gruppen induziert werden", *Math. Z.* 60 (1954), 274-286.

[8] Wolfgang Gaschütz, "Die Eulersche Funktion endlicher auflosbarer Gruppen", *Illinois J. Math.* 3 (1959), 469-476.

[9] Daniel Gorenstein, *Finite groups* (Harper and Row, New York, 1968).

[10] P. Hall, "The Eulerian functions of a group", *Quart. J. Math. Oxford* (1) 7 (1936), 134-151.

[11] G.H. Hardy, *Orders of infinity* (Cambridge Tracts in Mathematics and Mathematical Physics, 2nd Edition, Cambridge University Press, Cambridge, 1954).

[12] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers* (4th Edition, Oxford University Press, Oxford, 1960).

[13] Graham Higman, "Ordering by divisibility in abstract algebras", *Proc. London Math. Soc.*(3) 2 (1952), 326-336.

[14] Graham Higman, "Some remarks on varieties of groups", *Quart. J. Math. Oxford* (2) 10 (1959), 165-178.

[15] Graham Higman, "The orders of relatively free groups", *Proc. Internat. Conf. Theory of Groups*, Austral. Nat. Univ., Canberra, 1965 (Gordon and Breach, New York, 1967).

[16] B. Huppert, *Endliche Gruppen I* (Die Grundlehren der mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin, Heidelberg, New York, 1967).

[17] Konrad Knopp, *Theory and application of infinite series* (Blackie and Son Limited, London and Glasgow, 1951).

[18] Serge Lang, *Algebra* (Addison-Wesley, Reading, Massachusetts, 1965).

[19] B.H. Neumann, *Lectures on topics in the theory of infinite groups* (Tata Institute of Fundamental Research, Bombay, 1960).

[20] Hanna Neumann, *Varieties of groups* (Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 37. Springer-Verlag, Berlin, Heidelberg, New York, 1967).

[21] M.F. Newman, "On a class of nilpotent groups", *Proc. London Math. Soc.* (3) 10 (1960), 365-375.

[22] A.Ju. Ol'šanskiĭ, "On the problem of a finite basis for the identities of groups" (Russian), *Izv. Akad. Nauk SSSR Ser. Mat.* 34 (1970), 376-384.

[23] Marlene Schick, "On central decompositions of groups I, II", (preprint).

[24] C.Y. Tang, "On uniqueness of central decompositions of groups", *Pacific J. Math.* 33 (1970), 749-761.

[25] Seth Warner, *Modern Algebra II* (Prentice-Hall, Englewood Cliffs, New Jersey, 1965).

[26] David L. Winter, "The automorphism group of an extraspecial p-group", (preprint).